Unit E2

Quotient groups and conjugacy

Introduction

In the final section of the previous unit you met the idea of a *normal subgroup*. This next unit covers two topics that are both related to normal subgroups.

In the first section you will study *quotient groups*. You will see that if G is a group with a normal subgroup N then, in a sense that you will learn about, we can 'divide' G by N to obtain a *quotient group* G/N. Essentially, the group G can be 'broken down' into two groups N and G/N. You can think of the process as being similar to the way that if g is a natural number with a positive divisor n, then g can be broken down into the two numbers n and g/n: for example, the number 12 can be broken down into the numbers 4 and $12/4 = 3$.

In the other four sections you will learn how the idea of *conjugacy*, which you met in the context of symmetric groups in Unit B3 *Permutations*, can be generalised to all groups. As you will see, conjugacy can help us to understand the relationships between different elements of the same group. It also gives us useful methods for determining whether or not a subgroup of a group is a normal subgroup, and it can help us find more subgroups of a group once we know some subgroups.

This is a substantial unit, so you should expect to spend longer studying it than you would for a typical group theory unit. The next unit, Unit E3, is much shorter.

1 Quotient groups

In this section you will see that if G is a group with a normal subgroup N then we can form a new group whose elements are the cosets of N in G. We denote this group by G/N and call it a *quotient group* of G.

1.1 What is a quotient group?

Before you can learn more about quotient groups, you need to learn about the idea of *set composition* in a group. This is the binary operation of any quotient group of the group.

Given any group G, we can use its binary operation to obtain a related binary operation, known as set composition, that is defined on the set of *subsets* of G. That is, this new binary operation is a way of combining any two subsets of G to give another subset of G. It is defined below.

Definition

Let G be a group. Then the binary operation $\cdot$, called **set composition** in G, is defined on the set of subsets of G by

$$X \cdot Y = \{xy : x \in X,\ y \in Y\}$$

for all subsets X and Y of G.

That is, if X and Y are subsets of G then $X \cdot Y$ is the subset of G obtained by composing each element of X with each element of Y, in that order.

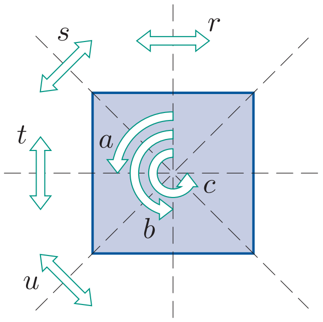


Figure 1 The symmetries of the square

Table 1 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

Worked Exercise E19

Determine the following composites of subsets in the group $S(\square)$.

(The non-identity symmetries of the square are shown in Figure 1 and the group table of $S(\square)$ is given as Table 1.)

(a) $\{s, u\} \cdot \{r, t\}$ (b) $\{b, t\} \cdot \{c, u\}$

Solution

(a)
$$\begin{aligned} \{s, u\} \cdot \{r, t\} &= \{s \circ r,\ s \circ t,\ u \circ r,\ u \circ t\} \\ &= \{a, c, c, a\} \\ &= \{a, c\} \end{aligned}$$

(b)
$$\begin{aligned} \{b, t\} \cdot \{c, u\} &= \{b \circ c,\ b \circ u,\ t \circ c,\ t \circ u\} \\ &= \{a, s, u, c\} \end{aligned}$$

Notice from Worked Exercise E19 that when we use set composition to combine two subsets of a group G we may obtain repeated elements. However, we write the resulting set with each element appearing just once, since a set does not contain repeated elements. The order in which we write the elements does not matter, since the elements of a set can be written in any order.

Exercise E49

Determine the following composites of subsets in $S(\square)$.

(a) $\{e, b\} \cdot \{r, t\}$ (b) $\{a, c\} \cdot \{a, c\}$ (c) $\{a, s\} \cdot \{a, s\}$

(d) $\{a, s\} \cdot \{a, s, e\}$

For an *additive* group G, we denote set composition by $+$ rather than $\cdot$, as illustrated in the next worked exercise.

Worked Exercise E20

Determine the composite of subsets $\{1,4,7\}+\{2,5,8\}$ in the group $\mathbb{Z}_9$.

Solution

$$\begin{aligned}\{1,4,7\}+\{2,5,8\} &= \{1+_9 2,\ 1+_9 5,\ 1+_9 8,\\ &\qquad 4+_9 2,\ 4+_9 5,\ 4+_9 8,\\ &\qquad 7+_9 2,\ 7+_9 5,\ 7+_9 8\}\\ &= \{3,6,0,6,0,3,0,3,6\}\\ &= \{0,3,6\}\end{aligned}$$

Exercise E50

Determine the following composites of subsets in the group $\mathbb{Z}_9$.

(a) $\{1,4,7\}+\{1,4,7\}$ (b) $\{0,3,6\}+\{1,4,7\}$

Set composition in an abelian group is a commutative binary operation, since for any two subsets X and Y of an abelian group we have

$$\begin{aligned}X\cdot Y &= \{xy : x\in X,\ y\in Y\}\\ &= \{yx : y\in Y,\ x\in X\}\\ &= Y\cdot X.\end{aligned}$$

On the other hand, set composition in a non-abelian group is a non-commutative binary operation, since a non-abelian group contains elements x and y such that $xy\neq yx$, and

$$\{x\}\cdot\{y\}=\{xy\}$$

whereas

$$\{y\}\cdot\{x\}=\{yx\}.$$

Exercise E51

Show that, in $S(\square)$,

$$\{b,t\}\cdot\{c,u\}\neq\{c,u\}\cdot\{b,t\}.$$

(The composite on the left here was found in Worked Exercise E19(b). The group table of $S(\square)$ is given as Table 2.)

Table 2 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

Although set composition is defined for any two subsets of a group, we will mainly be interested in applying it to *cosets of normal subgroups*. (You met the ideas of cosets and normal subgroups in Sections 4 and 5 of Unit E1 *Cosets and normal subgroups*.) Remember that for normal subgroups we refer simply to *cosets* rather than *left cosets* or *right cosets*, because for normal subgroups left cosets and right cosets are the same.

Let us look at what happens when we use set composition to compose two cosets of the same normal subgroup of a group.

Consider the example of the group $S(\square)$ and its normal subgroup $\{e, b\}$. You saw that this subgroup is normal in Worked Exercise E18 in Section 5 of Unit E1. We found there that its cosets are

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

Let us look at what happens when we use set composition to compose two of these four cosets.

For example, we have

$$\begin{aligned}\{a, c\} \cdot \{r, t\} &= \{a \circ r,\ a \circ t,\ c \circ r,\ c \circ t\}\\ &= \{s, u, u, s\}\\ &= \{s, u\}.\end{aligned}$$

This composite has turned out to be equal to one of the four cosets.

In fact we have already composed some other pairs of these four cosets. In Worked Exercise E19 and Exercise E49 we found that

$$\begin{aligned}&\{s, u\} \cdot \{r, t\} = \{a, c\},\\ &\{e, b\} \cdot \{r, t\} = \{r, t\},\\ &\{a, c\} \cdot \{a, c\} = \{e, b\}.\end{aligned}$$

Again, each of these composites is equal to one of the four cosets. In the next exercise you are asked to investigate whether composing a pair of the four cosets always gives one of the four cosets.

Exercise E52

(a) Complete the Cayley table below for the cosets of the normal subgroup $\{e, b\}$ of $S(\square)$ under set composition. The composites already entered are those given above and some others that have been worked out for you to save you time.

(The group table of $S(\square)$ is given as Table 3.)

$\cdot$	$\{e,b\}$	$\{a,c\}$	$\{r,t\}$	$\{s,u\}$
$\{e,b\}$		$\{a,c\}$	$\{r,t\}$	$\{s,u\}$
$\{a,c\}$	$\{a,c\}$	$\{e,b\}$	$\{s,u\}$	
$\{r,t\}$	$\{r,t\}$		$\{e,b\}$	$\{a,c\}$
$\{s,u\}$	$\{s,u\}$	$\{r,t\}$	$\{a,c\}$	

Table 3 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

(b) Check whether all the sets in the body of the table are cosets of $\{e, b\}$ in $S(\square)$.

Exercise E52 shows that composing a pair of cosets of $\{e, b\}$ in $S(\square)$ always gives a coset of $\{e, b\}$ in $S(\square)$: in other words, the set of cosets of $\{e, b\}$ in $S(\square)$ is closed under set composition.

In the next exercise you are asked to determine whether the set of cosets of the normal subgroup $\{0, 3, 6\}$ of the additive group $\mathbb{Z}_9$ is also closed under set composition. This set is a subgroup of $\mathbb{Z}_9$ because it is the cyclic subgroup generated by 3, and it is normal in $\mathbb{Z}_9$ because $\mathbb{Z}_9$ is abelian. (By Theorem E10 in Unit E1, every subgroup of an abelian group is normal.)

Exercise E53

(a) Complete the Cayley table below for the cosets of the normal subgroup $\{0, 3, 6\}$ of the group $\mathbb{Z}_9$ under set composition.

(The composites already entered were obtained in Worked Exercise E20 and Exercise E50. Remember that set composition in $\mathbb{Z}_9$ is commutative, because $\mathbb{Z}_9$ is abelian, so to complete the table you have to work out only three composites, not four.)

$+$	$\{0, 3, 6\}$	$\{1, 4, 7\}$	$\{2, 5, 8\}$
$\{0, 3, 6\}$		$\{1, 4, 7\}$	
$\{1, 4, 7\}$	$\{1, 4, 7\}$	$\{2, 5, 8\}$	$\{0, 3, 6\}$
$\{2, 5, 8\}$		$\{0, 3, 6\}$	

(b) Check whether all the sets in the body of the table are cosets of $\{0, 3, 6\}$ in $\mathbb{Z}_9$.

Exercises E52 and E53 seem to suggest that if N is a normal subgroup of a group G, then the set of cosets of N in G is always closed under set composition. This is indeed the case, as is confirmed by the theorem below. This theorem says that if we compose the coset of N that contains the element x with the coset of N that contains the element y, in that order, then we obtain the coset of N that contains the element xy.

Of course, if we compose the coset of N that contains the element x with the coset of N that contains the element y, in that order, then we will obtain a *set* that contains the element xy: this follows immediately from the definition of set composition. The significance of the theorem is that the set that we obtain is always a *coset* of N.

Theorem E14

Let N be a normal subgroup of a group G. Then, for all $x, y \in G$,

$$xN \cdot yN = (xy)N.$$

Proof Let $x, y \in G$. To show that the two sets $xN \cdot yN$ and $(xy)N$ are equal, we show that $xN \cdot yN \subseteq (xy)N$ and $(xy)N \subseteq xN \cdot yN$.

Proof that $xN \cdot yN \subseteq (xy)N$

Let $z \in xN \cdot yN$. Then

$$z = xn_1yn_2$$

for some $n_1, n_2 \in N$. We have to show that $z \in (xy)N$.

Consider the expression n_1y that occurs in the middle of the expression for z above. We know that $n_1y \in Ny$, and we know that $Ny = yN$, since N is a normal subgroup. Therefore $n_1y \in yN$. It follows that there is some element n_3, say, of N such that

$$n_1y = yn_3.$$

Using this equation to replace the expression n_1y in the expression for z above gives

$$z = xyn_3n_2.$$

Now $n_3n_2 \in N$, since N is a subgroup, so we can conclude that $z \in (xy)N$.

Hence $xN \cdot yN \subseteq (xy)N$.

Proof that $(xy)N \subseteq xN \cdot yN$

Let $z \in (xy)N$. Then

$$z = xyn$$

for some $n \in N$. Since $x \in xN$ and $yn \in yN$, it follows that

$$z \in xN \cdot yN.$$

Hence $(xy)N \subseteq xN \cdot yN$.

This completes the proof that $xN \cdot yN = (xy)N$. ■

So we now know the following fact:

> If N is a normal subgroup of a group G, then the set of cosets of N in G is closed under set composition.

Before we consider cosets of normal subgroups further, let us consider whether a similar fact might hold for subgroups that are *not normal*. Might it be true that if H is *any* subgroup of a group G, then the set of left cosets of H in G is always closed under set composition, and the set of right cosets of H in G is always closed under set composition? In fact this is not true, as you are asked to show in the next exercise. So Theorem E14 cannot be generalised to include subgroups that are not normal.

Exercise E54

The left cosets of the subgroup $\{e, r\}$ in the group $S(\square)$ are

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\},$$

and the right cosets are

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

Find counterexamples to show that the set of left cosets of $\{e, r\}$ is not closed under set composition in $S(\square)$, and neither is the set of right cosets.

(The cosets of the subgroup $\{e, r\}$ in $S(\square)$ were found in Worked Exercises E12 and E15 in Subsections 4.1 and 4.2 of Unit E1. The group table of $S(\square)$ is given as Table 4.)

Table 4 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

So far in this subsection we have found that if N is a normal subgroup of a group G, then the set of cosets of N in G is closed under set composition. In other words, it satisfies group axiom G1. In fact even more is true: the set of cosets with set composition also satisfies the other three group axioms and hence *is a group*. You will see a proof of this fact shortly, but first, to illustrate it, let us look again at the Cayley tables that you should have found in Exercises E52 and E53.

The Cayley table for the cosets of the normal subgroup $\{e, b\}$ in $S(\square)$ is as follows.

$\cdot$	$\{e, b\}$	$\{a, c\}$	$\{r, t\}$	$\{s, u\}$
$\{e, b\}$	$\{e, b\}$	$\{a, c\}$	$\{r, t\}$	$\{s, u\}$
$\{a, c\}$	$\{a, c\}$	$\{e, b\}$	$\{s, u\}$	$\{r, t\}$
$\{r, t\}$	$\{r, t\}$	$\{s, u\}$	$\{e, b\}$	$\{a, c\}$
$\{s, u\}$	$\{s, u\}$	$\{r, t\}$	$\{a, c\}$	$\{e, b\}$

In this table the row and column labelled by the coset $\{e, b\}$ both repeat the table borders. So the coset $\{e, b\}$ (this coset is the normal subgroup itself) is an identity element for set composition on the set of cosets. The table also shows that each coset has an inverse under set composition: in fact each coset is self-inverse, since the identity element $\{e, b\}$ appears in each position on the main diagonal. It is also true that set composition is associative; this follows from the fact that the original group operation is associative, as you will see proved formally shortly. So the Cayley table is a group table. The group in the Cayley table is isomorphic to the Klein four-group V, since it has order 4 and all its elements are self-inverse. (Distinguishing features for isomorphism classes of groups of orders 1 to 8 are given in Subsection 3.4 of Unit E1.)

Now let us look at the Cayley table for the cosets of the normal subgroup $\{0, 3, 6\}$ in the additive group $\mathbb{Z}_9$, which is as follows.

$+$	$\{0,3,6\}$	$\{1,4,7\}$	$\{2,5,8\}$
$\{0,3,6\}$	$\{0,3,6\}$	$\{1,4,7\}$	$\{2,5,8\}$
$\{1,4,7\}$	$\{1,4,7\}$	$\{2,5,8\}$	$\{0,3,6\}$
$\{2,5,8\}$	$\{2,5,8\}$	$\{0,3,6\}$	$\{1,4,7\}$

You can check in a similar way to the argument above that this Cayley table is a group table. Again the identity element is the normal subgroup itself, namely $\{0, 3, 6\}$ here. This time, however, the other elements are not self-inverse. The group in the table is isomorphic to the cyclic group C_3.

When we construct a Cayley table for a set of cosets, like those above, it is usually more convenient to denote the cosets by using notation of the form xN, rather than by listing the elements of each coset. If we do this for the two Cayley tables above, then we obtain the following tables.

The Cayley table for the cosets of $N = \{e, b\}$ in $S(\square)$ is as follows.

$\cdot$	N	aN	rN	sN
N	N	aN	rN	sN
aN	aN	N	sN	rN
rN	rN	sN	N	aN
sN	sN	rN	aN	N

The Cayley table for the cosets of $N = \{0, 3, 6\}$ in $\mathbb{Z}_9$ is as follows.

$+$	N	$1+N$	$2+N$
N	N	$1+N$	$2+N$
$1+N$	$1+N$	$2+N$	N
$2+N$	$2+N$	N	$1+N$

In Cayley tables like these, it is important to denote each coset in a consistent way throughout the table. For example, in the Cayley table for the cosets of $N = \{e, b\}$ in $S(\square)$, the coset $\{a, c\}$ could be written either as aN or cN, but it is important to choose one of these two possibilities and use it for every occurrence of the coset $\{a, c\}$ in the table. This makes the structure of the group clearer.

Now here is the proof that the cosets of a normal subgroup always form a group under set composition.

Theorem E15

Let N be a normal subgroup of a group G. Then the set of cosets of N in G, with the binary operation of set composition, is a group.

Proof We show that the set of cosets of N in G, with the binary operation of set composition, satisfies the four group axioms.

G1 Closure

By Theorem E14, the set of cosets of N in G is closed under set composition.

G2 Associativity

Let xN, yN and zN be any cosets of N in G. Then, by Theorem E14, and since the binary operation of G is associative,

$$xN \cdot (yN \cdot zN) = xN \cdot (yz)N = (x(yz))N = (xyz)N,$$

and

$$(xN \cdot yN) \cdot zN = (xy)N \cdot zN = ((xy)z)N = (xyz)N.$$

Since the two expressions obtained are the same, set composition is associative on the set of cosets of N in G.

G3 Identity

Let e be the identity element in G. Then, by Theorem E14, for each coset xN of N in G,

$$xN \cdot eN = (xe)N = xN,$$

and

$$eN \cdot xN = (ex)N = xN.$$

This shows that the coset eN, which is equal to N, is an identity element for set composition on the set of cosets of N in G.

G4 Inverses

Let xN be any coset of N in G. Since x is an element of the group G, it has an inverse element x^{-1} in G. Now, by Theorem E14,

$$xN \cdot x^{-1}N = (xx^{-1})N = eN = N,$$

and

$$x^{-1}N \cdot xN = (x^{-1}x)N = eN = N.$$

Since N is an identity element, this shows that $x^{-1}N$ is an inverse of xN with respect to set composition. Thus each coset of N has an inverse element in the set of cosets of N in G with respect to set composition.

Hence the set of cosets of N in G, with the binary operation of set composition, satisfies the four group axioms and so is a group. ■

The group formed by the cosets of a normal subgroup N of a group G is called the **quotient group** (or **factor group**) of G by N, and is denoted by G/N. In this context the notation G/N is pronounced as 'G modulo N' or 'G mod N' for short, or simply as 'G over N'.

If G is a *finite* group, then the number of cosets of N in G is $|G|/|N|$, since each coset of N contains the same number of elements as N, and hence the quotient group of G by N has order $|G|/|N|$. For example, as you have seen, the group formed by the cosets of $\{e, b\}$ in $S(\square)$ has order $8/2 = 4$, and the group formed by the cosets of $\{0, 3, 6\}$ in $\mathbb{Z}_9$ has order $9/3 = 3$.

More generally, for any group G, finite or infinite, and any normal subgroup N of G:

- if N has r cosets in G, then G/N has order r
- if N has infinitely many cosets in G, then G/N has infinite order.

In other words, the order of G/N is equal to the *index* of N in G.

Here is a summary of the important facts that we have established in this subsection.

Quotient groups

Let N be a normal subgroup of a group G. Then the set of cosets of N in G is a group under set composition, called the **quotient group** or **factor group** of G by N and denoted by G/N.

- Set composition of elements of G/N is given by

  $$xN \cdot yN = (xy)N \quad \text{for each } x, y \in G.$$

  If G is additive, then this is written as

  $$(x + N) + (y + N) = (x + y) + N \quad \text{for each } x, y \in G.$$

- The identity of G/N is N.
- For each $x \in G$, the inverse of xN is $x^{-1}N$.

  If G is additive, the inverse of $x + N$ is written as $-x + N$.

- If G is finite, then $|G/N| = |G|/|N|$.

You saw earlier that set composition in an abelian group is a commutative binary operation, and set composition in a non-abelian group is a non-commutative binary operation. It follows from the first of these facts that if N is a normal subgroup of an abelian group G, then the quotient group G/N is abelian.

If N is a normal subgroup of a *non-abelian* group G, then the quotient group G/N may be either abelian or non-abelian. This is because even though set composition is not commutative on the set of all *subsets* of G, it may be commutative on the set of all *cosets* of N in G. For example, the group $S(\square)$ is non-abelian but the quotient group $S(\square)/N$, where $N = \{e, b\}$, is abelian, as you can see if you look back at its Cayley table given earlier (for example, after Exercise E54).

As mentioned in the introduction to this unit, you can think of the process of forming a quotient group of a group G as a way of 'breaking G down' into two simpler groups N and G/N, just as dividing a natural number by a positive divisor breaks it down into two simpler numbers.

The concept of a quotient group emerged in the second half of the nineteenth century, although it took some time to evolve into the form in which we know it today. Several mathematicians contributed to its development, including Enrico Betti (1823–1892) and Camille Jordan (1838–1922). In addition, it is now known that Richard Dedekind (1831–1916) discovered the concept in the 1850s, but his work was unpublished. Evidence for this surfaced only in the 1970s, so his work had little influence. In 1889 the standard definition of a quotient group appeared in a paper by the German mathematician Otto Hölder (1859–1937) and from then on it began to appear in textbooks and monographs.

The term *factor group* also appears in Hölder's 1889 paper, though Hölder reserved it for a slightly different notion. The two terms, *quotient group* and *factor group*, were made synonymous in 1897 by the British group theorist William Burnside (1852–1927) after a misreading of Hölder, and both terms are now in common usage with Hölder's original distinction almost completely lost.

Otto Hölder

It is sometimes possible to observe a quotient group of a finite group in the group table of the original group. If G is a finite group with a normal subgroup N, and we arrange the elements in the row and column headings of the group table of G so that elements in the same coset of N are together, then the quotient group G/N becomes apparent as a 'blocking' of the group table.

For example, in the group table for $S(\square)$ on the left in Figure 2, the row and column headings have been arranged so that the elements of each of the cosets

$$\{e,b\}, \quad \{a,c\}, \quad \{r,t\}, \quad \{s,u\}$$

of the normal subgroup $N = \{e,b\}$ are together. To highlight the blocking, each coset has been assigned a colour, as indicated by the background colours of the row and column headings, and each element in the table has been given a background colour according to the coset in which it lies. The result is that the body of the table is split into a 4×4 array of 2×2 coloured blocks. Since each colour represents a coset, the coloured blocks form the group table of the quotient group $S(\square)/N$. This quotient group is shown on the right in Figure 2.

$\circ$	e	b	a	c	r	t	s	u
e	e	b	a	c	r	t	s	u
b	b	e	c	a	t	r	u	s
a	a	c	b	e	s	u	t	r
c	c	a	e	b	u	s	r	t
r	r	t	u	s	e	b	c	a
t	t	r	s	u	b	e	a	c
s	s	u	r	t	a	c	e	b
u	u	s	t	r	c	a	b	e

$S(\square)$

$\bullet$	N	aN	rN	sN
N	N	aN	rN	sN
aN	aN	N	sN	rN
rN	rN	sN	N	aN
sN	sN	rN	aN	N

$S(\square)/N$, where $N = \{e,b\}$

Figure 2 Blocking in the group table of $S(\square)$

Similarly, the group table for $\mathbb{Z}_9$ on the left in Figure 3 shows the quotient group formed by the cosets of the normal subgroup $\{0,3,6\}$. This quotient group is shown on the right in Figure 3.

$+$	0	3	6	1	4	7	2	5	8
0	0	3	6	1	4	7	2	5	8
3	3	6	0	4	7	1	5	8	2
6	6	0	3	7	1	4	8	2	5
1	1	4	7	2	5	8	3	6	0
4	4	7	1	5	8	2	6	0	3
7	7	1	4	8	2	5	0	3	6
2	2	5	8	3	6	0	4	7	1
5	5	8	2	6	0	3	7	1	4
8	8	2	5	0	3	6	1	4	7

$\mathbb{Z}_9$

$+$	N	$1+N$	$2+N$
N	N	$1+N$	$2+N$
$1+N$	$1+N$	$2+N$	N
$2+N$	$2+N$	N	$1+N$

$\mathbb{Z}_9/N$, where $N = \{0,3,6\}$

Figure 3 Blocking in the group table of $\mathbb{Z}_9$

In contrast, if H is a subgroup that is not normal in a finite group G, and we arrange the elements in the row and column headings of the group table of G so that the elements in the left cosets or right cosets of H are together, then there is no similar blocking effect. For example, in the group table for $S(\square)$ in Figure 4, the row and column headings have been arranged in order of the left cosets of the subgroup $\{e, r\}$ of the group $S(\square)$, which are

$$\{e,r\}, \quad \{a,s\}, \quad \{b,t\}, \quad \{c,u\}.$$

The resulting coloured blocks, and hence the left cosets, do not form the Cayley table of a group.

$\circ$	e	r	a	s	b	t	c	u
e	e	r	a	s	b	t	c	u
r	r	e	u	c	t	b	s	a
a	a	s	b	t	c	u	e	r
s	s	a	r	e	u	c	t	b
b	b	t	c	u	e	r	a	s
t	t	b	s	a	r	e	u	c
c	c	u	e	r	a	s	b	t
u	u	c	t	b	s	a	r	e

$S(\square)$

Figure 4 Failure to block in the group table of $S(\square)$

You saw in Unit B1 *Symmetry and groups* that if F is a figure whose symmetry group $S(F)$ is finite and contains indirect symmetries, then the group table of $S(F)$ can be blocked into direct symmetries and indirect symmetries. This is a special case of the blocking into cosets described above, because the direct symmetries form a subgroup $S^+(F)$, which is a normal subgroup since it has index 2 in $S(F)$, and the indirect symmetries form the other coset of $S^+(F)$ in $S(F)$. (Any subgroup of index 2 is normal by Theorem E11 in Unit E1.) For example, Figure 5 shows the group table for $S(\square)$ blocked in this way.

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

$S(\square)$

Figure 5 Blocking of $S(\square)$ into direct symmetries and indirect symmetries

If G is a group with a normal subgroup N, then it can be useful to identify the structure of the quotient group G/N by finding a standard, familiar group to which this quotient group is isomorphic. Here is an example.

Worked Exercise E21

Consider the subgroup $N = \langle 4 \rangle$ of the group U_{15}.

(a) List the elements of the group U_{15}.

(b) Find the elements of the subgroup N, and explain why N is normal in U_{15}.

(c) Find the cosets of N in U_{15}.

(d) Construct the group table of the quotient group U_{15}/N.

(e) State the identity element of this quotient group, and state the inverse of each of its elements.

(f) State a standard group that is isomorphic to this quotient group.

Solution

(a) The elements of U_{15} are all the numbers in $\mathbb{Z}_{15}$ that are coprime to 15.

We have

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

(b) The subgroup $N = \langle 4 \rangle$ is the cyclic subgroup of U_{15} generated by 4, so its elements are all the powers of 4 in U_{15}. The binary operation of U_{15} is $\times_{15}$.

In $\mathbb{Z}_{15}$ we have

$$4^2 = 4 \times_{15} 4 = 1,$$

so 4 has order 2 and hence $N = \langle 4 \rangle = \{1, 4\}$. This subgroup of U_{15} is normal in U_{15} because U_{15} is abelian.

(c) To find the cosets of N in U_{15}, use Strategy E1 from Unit E1. That is, repeatedly choose an element x of U_{15} not yet assigned to a coset and find the coset containing x, until all the elements of U_{15} have been assigned to cosets.

The cosets are

$$\begin{aligned} N &= \{1, 4\}, \\ 2N &= \{2 \times_{15} 1,\ 2 \times_{15} 4\} = \{2, 8\}, \\ 7N &= \{7 \times_{15} 1,\ 7 \times_{15} 4\} = \{7, 13\}, \\ 11N &= \{11 \times_{15} 1,\ 11 \times_{15} 4\} = \{11, 14\}. \end{aligned}$$

(d) To find the entries of the group table of U_{15}/N use Theorem E14, which gives

$$xN \cdot yN = (x \times_{15} y)N \quad \text{for all } x, y \in U_{15}.$$

Remember to denote each coset consistently, as one of N, $2N$, $7N$, $11N$. For example,

$$2N \cdot 7N = (2 \times_{15} 7)N = 14N = 11N.$$

The group table of U_{15}/N is as follows.

$\cdot$	N	$2N$	$7N$	$11N$
N	N	$2N$	$7N$	$11N$
$2N$	$2N$	N	$11N$	$7N$
$7N$	$7N$	$11N$	N	$2N$
$11N$	$11N$	$7N$	$2N$	N

(e) The identity element of U_{15}/N is N. Each element is self-inverse.

(f) To find a standard group isomorphic to U_{15}/N, use the table of isomorphism classes near the end of Subsection 3.4 in Unit E1.

The group U_{15}/N has four elements and each element is self-inverse, so it is isomorphic to the Klein four-group V.

Here is a summary of the strategy used in Worked Exercise E21.

Strategy E3

To find a group isomorphic to a finite quotient group G/N where N is a normal subgroup of the group G, do the following.

1. Determine the cosets of N in G, by repeatedly choosing an element x of G not yet assigned to a coset and finding the coset xN (or $x + N$, if G is additive) until all the elements of G have been assigned to cosets.
2. Construct the group table of G/N by composing each pair of cosets using the rule

   $$xN \cdot yN = (xy)N$$

   (or

   $$(x + N) + (y + N) = (x + y) + N$$

   if G is additive).

   Make sure to use just one way to write each coset.
3. By inspection of the group table, and possibly using the table of isomorphism classes for small groups, identify a standard group isomorphic to G/N.

Exercise E55

Consider the subgroup $N = \langle 4 \rangle$ of $\mathbb{Z}_{17}^*$.

(a) Find the elements of N, and explain why it is normal in $\mathbb{Z}_{17}^*$.

(b) Find the cosets of N in $\mathbb{Z}_{17}^*$.

(c) Construct the group table of the quotient group $\mathbb{Z}_{17}^*/N$.

(d) State the identity element of this quotient group, and state the inverse of each of its elements.

(e) State a standard group that is isomorphic to this quotient group.

Exercise E56

Consider the subgroup $H = \langle 6 \rangle$ of the (additive) group $\mathbb{Z}_{12}$.

(a) Find the elements of H, and explain why it is normal in $\mathbb{Z}_{12}$.

(b) Find the cosets of N in $\mathbb{Z}_{12}$.

(c) Construct the group table of the quotient group $\mathbb{Z}_{12}/H$.

(d) State the identity element of this quotient group, and state the inverse of each of its elements.

(e) State a standard group that is isomorphic to this quotient group.

Exercise E57

The following table is the group table of a group G.

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	e	a	g	h	d	f
c	c	b	a	e	h	g	f	d
d	d	f	g	h	e	a	b	c
f	f	d	h	g	a	e	c	b
g	g	h	d	f	b	c	e	a
h	h	g	f	d	c	b	a	e

Consider the subset $N = \{e, a\}$ of G.

(a) Explain why N is a subgroup of G, and why it is normal in G.

(b) Find the cosets of N in G.

(c) Construct the group table of the quotient group G/N.

(d) State the identity element of this quotient group, and state the inverse of each of its elements.

(e) State a standard group that is isomorphic to this quotient group.

Exercise E58

The following table is the group table of a group G.

	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	r	q	t	s
q	q	s	e	t	p	r
r	r	t	p	s	e	q
s	s	q	t	e	r	p
t	t	r	s	p	q	e

Consider the subset $N = \{e, r, s\}$ of G.

(a) Explain why N is a subgroup of G, and why it is normal in G.

(b) Find the cosets of N in G.

(c) Construct the group table of the quotient group G/N.

(d) State the identity element of this quotient group, and state the inverse of each of its elements.

(e) State a standard group that is isomorphic to this quotient group.

1.2 Quotient groups of infinite groups

In all the examples of quotient groups G/N in the previous subsection, the group G was finite. In this subsection you will meet some quotient groups G/N where the group G is infinite. In this situation the quotient group G/N may be either finite or infinite, depending on whether the normal subgroup N has finitely many or infinitely many cosets in G.

We will begin by looking at some examples where the normal subgroup has finitely many cosets, so the quotient group is finite. All the examples of this type that we will look at are quotient groups of the infinite additive group $(\mathbb{Z}, +)$, which we will mostly denote simply by $\mathbb{Z}$.

Quotient groups of $(\mathbb{Z}, +)$

Consider the group $\mathbb{Z}$. This group is cyclic (it is generated by 1, for example), so all of its subgroups are cyclic, by Theorem B36 in Unit B2 *Subgroups and isomorphisms*. Since it is an additive group, if n is one of its elements then the cyclic subgroup $\langle n \rangle$ generated by n is given by

$$\langle n \rangle = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}.$$

Recall that we denote this subgroup by $n\mathbb{Z}$.

Since $\mathbb{Z}$ is an abelian group, all of its subgroups are normal. So the quotient group $\mathbb{Z}/n\mathbb{Z}$ exists for each integer n.

In the worked exercise below, all the elements of the particular quotient group $\mathbb{Z}/5\mathbb{Z}$ are found; in the exercise that follows you are asked to do the same for $\mathbb{Z}/4\mathbb{Z}$.

Worked Exercise E22

Find all the elements of the quotient group $\mathbb{Z}/5\mathbb{Z}$. Hence state the order of this group.

Solution

The elements of $\mathbb{Z}/5\mathbb{Z}$ are the cosets of $5\mathbb{Z}$ in $\mathbb{Z}$.

To find these cosets, we use Strategy E1 from Unit E1: we repeatedly choose an element x of $\mathbb{Z}$ not yet assigned to a coset and find the coset containing x, until all the elements of $\mathbb{Z}$ have been assigned to cosets.

The cosets are

$$\begin{aligned}
5\mathbb{Z} &= \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\},\\
1 + 5\mathbb{Z} &= \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\},\\
2 + 5\mathbb{Z} &= \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\},\\
3 + 5\mathbb{Z} &= \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\},\\
4 + 5\mathbb{Z} &= \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}.
\end{aligned}$$

These five cosets between them contain every element of $\mathbb{Z}$, so there are no more cosets.

Hence $\mathbb{Z}/5\mathbb{Z}$ has order 5.

Exercise E59

Find the elements of the quotient group $\mathbb{Z}/4\mathbb{Z}$. Hence state the order of this group.

In the next worked exercise and the exercise that follows we will construct group tables for the quotient groups $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

Worked Exercise E23

Construct a group table for the quotient group $\mathbb{Z}/5\mathbb{Z}$.

Solution

By Worked Exercise E22, the elements of $\mathbb{Z}/5\mathbb{Z}$ are the five cosets

$$5\mathbb{Z},\quad 1+5\mathbb{Z},\quad 2+5\mathbb{Z},\quad 3+5\mathbb{Z},\quad 4+5\mathbb{Z}.$$

Since $\mathbb{Z}$ is an additive group, the rule for set composition of these cosets is

$$(a+5\mathbb{Z}) + (b+5\mathbb{Z}) = (a+b)+5\mathbb{Z} \quad \text{for all } a,b \in \mathbb{Z}.$$

We make sure to express each coset in the table in just one way, as one of $5\mathbb{Z}$, $1+5\mathbb{Z}$, $2+5\mathbb{Z}$, $3+5\mathbb{Z}$ and $4+5\mathbb{Z}$.

For example,

$$\begin{aligned}
&(1+5\mathbb{Z}) + (2+5\mathbb{Z}) = 3+5\mathbb{Z},\\
&(4+5\mathbb{Z}) + (2+5\mathbb{Z}) = 6+5\mathbb{Z} = 1+5\mathbb{Z} \quad (\text{since } 6 \in 1+5\mathbb{Z}),\\
&5\mathbb{Z} + (4+5\mathbb{Z}) = (0+5\mathbb{Z}) + (4+5\mathbb{Z}) = 4+5\mathbb{Z}.
\end{aligned}$$

We work out all the composites needed for the table in this way.

The group table of $\mathbb{Z}/5\mathbb{Z}$ is

$+$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
$1+5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$
$2+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$
$3+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$
$4+5\mathbb{Z}$	$4+5\mathbb{Z}$	$5\mathbb{Z}$	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$

Exercise E60

Construct a group table for the quotient group $\mathbb{Z}/4\mathbb{Z}$.

Now look again at the group table for the quotient group $\mathbb{Z}/5\mathbb{Z}$, found in Worked Exercise E23. If we delete every occurrence of '$+5\mathbb{Z}$' (writing each occurrence of the coset $5\mathbb{Z}$ as $0+5\mathbb{Z}$ before doing so), then we obtain the following table.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

This is the group table for the group $\mathbb{Z}_5$.

This tells us that the quotient group $\mathbb{Z}/5\mathbb{Z}$ is isomorphic to the group $\mathbb{Z}_5$, and the following mapping is an isomorphism:

$$\begin{aligned}\phi : \mathbb{Z}/5\mathbb{Z} &\longrightarrow \mathbb{Z}_5\\ a+5\mathbb{Z} &\longmapsto a, \quad \text{for } a=0,1,2,3,4.\end{aligned}$$

If you look at your answer to Exercise E60, you will see that, similarly, if we delete every occurrence of '$+4\mathbb{Z}$' from the group table of the quotient group $\mathbb{Z}/4\mathbb{Z}$ (writing each occurrence of the coset $4\mathbb{Z}$ as $0+4\mathbb{Z}$ before doing so), then we obtain the group table for the group $\mathbb{Z}_4$. Hence the quotient group $\mathbb{Z}/4\mathbb{Z}$ is isomorphic to the group $\mathbb{Z}_4$.

Exercise E61

Write down an isomorphism from the quotient group $\mathbb{Z}/4\mathbb{Z}$ to the group $\mathbb{Z}_4$.

In general the theorem below holds. The proof of this theorem is not an important one for you to read: it is a little technical and the general ideas of the proof should be apparent to you from the particular examples $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ above. But read it if you want to see a formal proof.

Theorem E16

For each integer $n \geq 2$, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the group $\mathbb{Z}_n$, and the following mapping is an isomorphism:

$$\begin{aligned}\phi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}_n\\ a+n\mathbb{Z} &\longmapsto a, \quad \text{for } a=0,1,2,\dots,n-1.\end{aligned}$$

Proof Let n be an integer with $n \geq 2$. First we show that the distinct cosets of $n\mathbb{Z}$ are

$$0+n\mathbb{Z}, \quad 1+n\mathbb{Z}, \quad 2+n\mathbb{Z}, \quad \dots, \quad (n-1)+n\mathbb{Z}.$$

For any elements $a, b \in \mathbb{Z}$, we have

$$\begin{aligned} a + n\mathbb{Z} = b + n\mathbb{Z} &\iff a \in b + n\mathbb{Z} \\ &\iff a = b + nr \quad \text{for some } r \in \mathbb{Z} \\ &\iff a \equiv b \pmod{n}. \end{aligned}$$

That is, two cosets $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ are equal if and only if a and b are congruent modulo n. It follows that the distinct cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are the n cosets listed above.

Next we show that the mapping ϕ specified in the statement of the theorem is an isomorphism. It follows from what we have just proved that ϕ is one-to-one and onto. It remains to prove that for all $a, b \in \{0, 1, \ldots, n-1\}$,

$$\phi\big((a + n\mathbb{Z}) + (b + n\mathbb{Z})\big) = \phi(a + n\mathbb{Z}) +_n \phi(b + n\mathbb{Z}).$$

Let $a, b \in \{0, 1, \ldots, n-1\}$ and let $c = a +_n b$. Then

$$\begin{aligned} &\phi\big((a + n\mathbb{Z}) + (b + n\mathbb{Z})\big) \\ &= \phi\big((a+b) + n\mathbb{Z}\big) \quad \text{(by the rule for set composition of cosets of } n\mathbb{Z}) \\ &= \phi(c + n\mathbb{Z}) \quad (\text{since } a + b \equiv c \pmod{n}, \text{ so } (a+b) + n\mathbb{Z} = c + n\mathbb{Z}) \\ &= c \quad (\text{by the rule of } \phi). \end{aligned}$$

Also

$$\begin{aligned} &\phi(a + n\mathbb{Z}) +_n \phi(b + n\mathbb{Z}) \\ &= a +_n b \quad (\text{by the rule of } \phi) \\ &= c. \end{aligned}$$

Hence the required equation holds. This completes the proof. ■

We can use Theorem E16 to deduce facts about a quotient group $\mathbb{Z}/n\mathbb{Z}$ from facts that we know about the group $\mathbb{Z}_n$. For example, since $\mathbb{Z}_n$ is a cyclic group of order n, Theorem E16 tells us that the quotient group $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n.

You are asked to use Theorem E16 in this way in the next exercise. You will need to use the result that if $\phi : (G, \circ) \longrightarrow (H, *)$ is an isomorphism, then g is a generator of $(G, \circ)$ if and only if $\phi(g)$ is a generator of $(H, *)$. This follows from Theorem B46 in Unit B2, which states that if $\phi : (G, \circ) \longrightarrow (H, *)$ is an isomorphism, then an element $g \in (G, \circ)$ and its image $\phi(g) \in (H, *)$ either both have the same finite order or both have infinite order. Remember that the generators of $\mathbb{Z}_n$ are the integers in $\mathbb{Z}_n$ that are coprime to n. (See Corollary B40 in Unit B2.)

Exercise E62

Find all the generators of each of the following quotient groups.

(a) $\mathbb{Z}/6\mathbb{Z}$ (b) $\mathbb{Z}/4\mathbb{Z}$ (c) $\mathbb{Z}/5\mathbb{Z}$

The quotient group $\mathbb{R}/\mathbb{Z}$

We now consider an example of a quotient group G/N for which not only is G an infinite group, but also G/N is an infinite group. In other words, the normal subgroup N has infinitely many cosets in G. We will look at just a single example of such a quotient group here, namely the quotient group $\mathbb{R}/\mathbb{Z}$, where $\mathbb{R}$ and $\mathbb{Z}$ denote the additive groups $(\mathbb{R},+)$ and $(\mathbb{Z},+)$.

The quotient group $\mathbb{R}/\mathbb{Z}$ certainly exists, because $\mathbb{R}$ is an abelian group, and hence its subgroup $\mathbb{Z}$ is normal.

The elements of the quotient group $\mathbb{R}/\mathbb{Z}$ are the cosets of $\mathbb{Z}$ in $\mathbb{R}$. For any real number $x \in \mathbb{R}$, the coset to which x belongs is

$$\begin{aligned} x+\mathbb{Z} &= x+\{\dots,-2,-1,0,1,2,\dots\}, \\ &= \{\dots,\ x-2,\ x-1,\ x,\ x+1,\ x+2,\ \dots\}. \end{aligned}$$

Here are some examples of such cosets:

$$\begin{aligned} 1+\mathbb{Z} &= \{\dots,\ 1-2,\ 1-1,\ 1,\ 1+1,\ 1+2,\ \dots\} \\ &= \{\dots,\ -1,\ 0,\ 1,\ 2,\ 3,\ \dots\} \\ &= \mathbb{Z}, \\ 1.6+\mathbb{Z} &= \{\dots,\ 1.6-2,\ 1.6-1,\ 1.6,\ 1.6+1,\ 1.6+2,\ \dots\} \\ &= \{\dots,\ -0.4,\ 0.6,\ 1.6,\ 2.6,\ 3.6,\ \dots\}, \\ 2.6+\mathbb{Z} &= \{\dots,\ 2.6-2,\ 2.6-1,\ 2.6,\ 2.6+1,\ 2.6+2,\ \dots\} \\ &= \{\dots,\ 0.6,\ 1.6,\ 2.6,\ 3.6,\ 4.6,\ \dots\}. \end{aligned}$$

Of course, different values of x can give the same coset $x+\mathbb{Z}$. For instance, the examples above show that

$$1.6+\mathbb{Z} = 2.6+\mathbb{Z}.$$

Exercise E63

Consider the following list of five cosets of $\mathbb{Z}$ in $\mathbb{R}$:

$$0.2+\mathbb{Z},\quad 1.2+\mathbb{Z},\quad 3.7+\mathbb{Z},\quad -1.3+\mathbb{Z},\quad -4.8+\mathbb{Z}.$$

(a) Find each of these cosets. (As in the examples above, list enough elements of each coset to make the full infinite list of elements clear.)

(b) How many different cosets are there in the list?

To help us understand the structure of $\mathbb{R}/\mathbb{Z}$, it is useful to express each coset of $\mathbb{Z}$ in $\mathbb{R}$ in a single, consistent way, just as we did for the cosets in each quotient group that we considered earlier.

To see how we might do this, observe that each coset $x+\mathbb{Z}$ of $\mathbb{Z}$ in $\mathbb{R}$ consists of the set $\mathbb{Z}$ shifted (by x) along the real line, as illustrated in Figure 6.

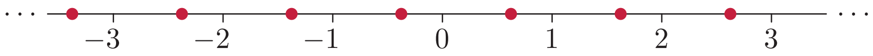


Figure 6 The elements of a coset $x+\mathbb{Z}$

Thus each coset contains exactly one real number in the interval $[0, 1)$.

For example, the coset $1.2 + \mathbb{Z}$, shown in Figure 7, contains the real number $0.2 \in [0, 1)$.

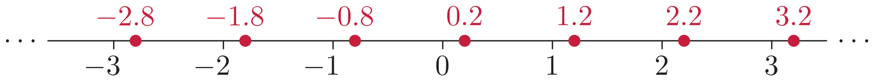


Figure 7 The elements of the coset $1.2 + \mathbb{Z}$

Similarly, the coset $-1.3 + \mathbb{Z}$, shown in Figure 8, contains the real number $0.7 \in [0, 1)$.

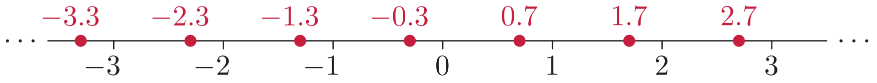


Figure 8 The elements of the coset $-1.3 + \mathbb{Z}$

This gives us a way to write each coset of $\mathbb{Z}$ in $\mathbb{R}$ in a single, consistent way: we write it in the form $x + \mathbb{Z}$ where $x \in [0, 1)$. For example, we write the coset $1.2 + \mathbb{Z}$ as $0.2 + \mathbb{Z}$, and the coset $-1.3 + \mathbb{Z}$ as $0.7 + \mathbb{Z}$, and so on.

Exercise E64

Write each of the following cosets of $\mathbb{Z}$ in $\mathbb{R}$ in the form $x + \mathbb{Z}$ where $x \in [0, 1)$.

(a) $3.1 + \mathbb{Z}$ (b) $-0.22 + \mathbb{Z}$ (c) $-3.1 + \mathbb{Z}$

Notice that to express a coset $y + \mathbb{Z}$ of $\mathbb{Z}$ in $\mathbb{R}$ in the form $x + \mathbb{Z}$ where $x \in [0, 1)$ we take $x = \operatorname{frac}(y)$, where $\operatorname{frac}(y)$ is the *fractional part* of y. Remember from Unit E1 that the **fractional part** $\operatorname{frac}(x)$ of a real number x is given by

$$\operatorname{frac}(x) = x - \lfloor x \rfloor,$$

where $\lfloor x \rfloor$ is the integer part of x (the largest integer that is less than or equal to x). Essentially, $\operatorname{frac}(x)$ is equal to 0 if x is an integer, and is equal to the distance from x to 'the next integer down' otherwise, as illustrated in Figure 9.

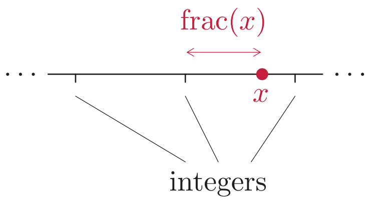


Figure 9 The fractional part of a real number x

For example, we write

$$1.2 + \mathbb{Z} \text{ as } 0.2 + \mathbb{Z} \text{ because } \operatorname{frac}(1.2) = 0.2,$$

$$-1.3 + \mathbb{Z} \text{ as } 0.7 + \mathbb{Z} \text{ because } \operatorname{frac}(-1.3) = 0.7,$$

$$1 + \mathbb{Z} \text{ as } 0 + \mathbb{Z} = \mathbb{Z} \text{ because } \operatorname{frac}(1) = 0.$$

We now have a helpful way to express the elements of the quotient group $\mathbb{R}/\mathbb{Z}$, so we turn to looking at how these elements are composed in $\mathbb{R}/\mathbb{Z}$. They are cosets, so we compose them using set composition. Since $\mathbb{R}$ is an additive group, the rule for set composition of cosets of $\mathbb{Z}$ in $\mathbb{R}$ is

$$(x+\mathbb{Z}) \mathbin{\boldsymbol{+}} (y+\mathbb{Z}) = (x+y)+\mathbb{Z}.$$

We make sure to express each composite in the form $x+\mathbb{Z}$ where $x \in [0,1)$.

For example,

$$\begin{aligned}(0.25+\mathbb{Z}) \mathbin{\boldsymbol{+}} (0.7+\mathbb{Z}) &= 0.95+\mathbb{Z},\\ (0.3+\mathbb{Z}) \mathbin{\boldsymbol{+}} (0.96+\mathbb{Z}) &= 1.26+\mathbb{Z} = 0.26+\mathbb{Z}.\end{aligned}$$

Consider the effect of deleting the occurrences of '$+\mathbb{Z}$' in the calculations above (and replacing the symbol $\boldsymbol{+}$ for set composition with the words 'composed with'):

$$\begin{aligned}&0.25 \text{ composed with } 0.7 = 0.95,\\ &0.3 \text{ composed with } 0.96 = 0.26.\end{aligned} \tag{1}$$

These calculations may remind you of calculations involving the binary operation $+_1$, which you met in Subsection 1.1 of Unit E1. Recall that this binary operation is defined on the interval $[0,1)$ by

$$x +_1 y = \operatorname{frac}(x+y).$$

So, for example,

$$\begin{aligned}&0.25 +_1 0.7 = 0.95,\\ &0.3 +_1 0.96 = 0.26.\end{aligned} \tag{2}$$

Equations (1) and equations (2) illustrate the fact that to compose two elements $x+\mathbb{Z}$ and $y+\mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$, where $x, y \in [0,1)$, we compose the numbers x and y using the binary operation $+_1$.

Exercise E65

Determine the following composites of cosets in the group $\mathbb{R}/\mathbb{Z}$.

(a) $(0.9+\mathbb{Z}) \mathbin{\boldsymbol{+}} (0.8+\mathbb{Z})$ (b) $(0.2+\mathbb{Z}) \mathbin{\boldsymbol{+}} \mathbb{Z}$

(c) $(0.5+\mathbb{Z}) \mathbin{\boldsymbol{+}} (0.7+\mathbb{Z}) \mathbin{\boldsymbol{+}} (0.8+\mathbb{Z})$

You might remember that the interval $[0,1)$ is a group under the binary operation $+_1$: you were asked to prove this in Exercise E2 in Subsection 1.1 of Unit E1.

You have now seen that every element of $\mathbb{R}/\mathbb{Z}$ corresponds to a unique element of the interval $[0,1)$, and that to compose two elements of $\mathbb{R}/\mathbb{Z}$ we compose the corresponding two elements of $[0,1)$ using the binary operation $+_1$. This tells us that the group $(\mathbb{R}/\mathbb{Z}, \boldsymbol{+})$ is isomorphic to the group $([0,1), +_1)$, as stated in the theorem below. The proof of this theorem is not an important proof for you to read: as with the proof of Theorem E16, the general ideas of the proof should be apparent from the discussion above.

Theorem E17

The quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the group $([0,1),+_1)$, and the following mapping is an isomorphism:

$$\begin{aligned}\phi : \mathbb{R}/\mathbb{Z} &\longrightarrow [0,1)\\ x+\mathbb{Z} &\longmapsto x, \quad \text{for } x \in [0,1).\end{aligned}$$

Proof We have seen that the distinct cosets of $\mathbb{Z}$ in $\mathbb{R}$ are given by

$$x+\mathbb{Z} \quad \text{where } x \in [0,1).$$

It follows that the mapping specified in the statement of the theorem is one-to-one and onto. It remains to prove that for all $x, y \in [0,1)$,

$$\phi((x+\mathbb{Z}) + (y+\mathbb{Z})) = \phi(x+\mathbb{Z}) +_1 \phi(y+\mathbb{Z}).$$

Let $x, y \in [0,1)$ and let $z = x +_1 y$. Then

$$\begin{aligned}&\phi((x+\mathbb{Z}) + (y+\mathbb{Z}))\\ &= \phi((x+y)+\mathbb{Z}) \quad \text{(by the rule for set composition of cosets of } \mathbb{Z} \text{ in } \mathbb{R})\\ &= \phi(z+\mathbb{Z}) \quad (\text{since } x +_1 y = z, \text{ so } (x+y)+\mathbb{Z} = z+\mathbb{Z})\\ &= z \quad (\text{by the rule of } \phi),\end{aligned}$$

and

$$\begin{aligned}&\phi(x+\mathbb{Z}) +_1 \phi(y+\mathbb{Z})\\ &= x +_1 y \quad (\text{by the rule of } \phi)\\ &= z.\end{aligned}$$

Hence the required equation holds. This completes the proof. ■

In the next exercise you might find it helpful to use Theorem E17 along with the fact that if $\phi : (G, \circ) \longrightarrow (H, *)$ is an isomorphism then an element $g \in (G, \circ)$ and its image $\phi(g) \in (H, *)$ either both have the same finite order or both have infinite order (Theorem B46 from Unit B2).

Exercise E66

(a) Find the order of the element $0.25 + \mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$, and write down the elements of the cyclic subgroup generated by this element.

(b) For each of the following possible orders of elements of $\mathbb{R}/\mathbb{Z}$, write down an element of $\mathbb{R}/\mathbb{Z}$ with that order.

(i) 5 (ii) 2 (iii) 3 (iv) 1

1.3 Simple groups (optional)

In this optional subsection you can learn about the idea of a *simple group*, which is extremely important in advanced group theory.

You have seen that every group of order 2 or more has at least two normal subgroups, namely itself and its trivial subgroup $\{e\}$. A group of order 2 or more that has no normal subgroups other than these two is called a simple group.

Definition

A group G of order 2 or more is **simple** if it has no proper non-trivial normal subgroups.

If G is a simple group, then the only quotient groups of G are

- the group $G/\{e\}$, which is isomorphic to G (because each coset of $\{e\}$ in G contains only one element)
- the group G/G, which is isomorphic to $\{e\}$ (because the only coset of G in G is G itself, which is the identity element of G/G).

As you saw in Subsection 1.1, we can think of the process of forming the quotient group of a group G by a normal subgroup N as a way of 'breaking down' G into the two simpler groups N and G/N, just as dividing a natural number by a positive divisor breaks it down into two 'simpler' numbers. But if G is simple, then we *cannot* break it down into simpler groups in this way – if we try, then the only groups that we obtain are the group $\{e\}$ and G itself.

If we pursue the analogy with the natural numbers, then the simple groups are rather like the prime numbers, whose only positive divisors are 1 and the number itself. Moreover, just as the prime numbers are the basic building blocks of the natural numbers, so the simple groups can be thought of as the basic building blocks of all groups. For this reason, it is of considerable importance in group theory to know which groups are simple. Both finite and infinite groups can be simple, but here we will consider only finite simple groups.

Here is an exercise to get you thinking about which finite groups might be simple.

Exercise E67

Determine whether the following groups are simple. (The non-identity elements of $S(\square)$ are shown in Figure 10.)

(a) $S(\square)$ (b) $\mathbb{Z}_6$ (c) $\mathbb{Z}_7$

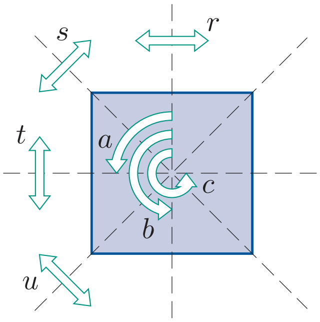


Figure 10 $S(\square)$

It turns out to be relatively straightforward to show which finite *abelian* groups are simple. You saw examples that illustrate the next result in Exercise E67(b) and (c).

Theorem E18

Let G be a finite abelian group. Then G is simple if and only if it is a cyclic group of prime order.

Proof

'If' part

Suppose that G is a cyclic group of prime order, p say. Then, by Lagrange's Theorem, the order of any subgroup of G is either 1 or p. It follows that the only subgroups of G are $\{e\}$ and G, so G is simple.

'Only if' part

Suppose that G is simple. Then the order of G is at least 2. Let x be any element of G other than the identity element. Since G is abelian, the cyclic subgroup $\langle x\rangle$ generated by x is normal in G, by Theorem E10 in Unit E1. Since G is simple it follows that $\langle x\rangle = G$, so G is cyclic.

Now suppose that the order n of the element x (and hence the order of G) is a *not* a prime number. Then $n = rs$, say, where r and s are integers such that $1 < r$, $s < n$. It follows that the element x^r has order s, because

$$(x^r)^s = x^{rs} = x^n = e$$

whereas if t is an integer such that $1 \leq t < s$ then

$$(x^r)^t \neq e,$$

because otherwise we would have $x^{rt} = e$, which is not true because x has order n and $1 < rt < rs = n$. Thus the cyclic subgroup $\langle x^r\rangle$ generated by x^r has order s. Since $1 < s < n$, this shows that $\langle x^r\rangle$ is a proper non-trivial normal subgroup of G, which is a contradiction because G is simple. It follows that G is a cyclic group of prime order. ■

Theorem E18 gives a complete answer to the question 'Which finite abelian groups are simple?' Let us now briefly consider some finite *non-abelian* groups.

You have met several standard families of such groups, as follows.

- The symmetry groups of regular polygons, such as $S(\triangle)$, $S(\square)$, $S(\text{⬠})$, and so on, which are all non-abelian. These groups are called the *dihedral groups* of orders 6, 8, 10, and so on.
- The symmetric groups S_n, which are non-abelian for $n \geq 3$.
- The alternating groups A_n, which are non-abelian for $n \geq 4$.

It is straightforward to check that all these groups *are* non-abelian, as follows. In a dihedral group $S(F)$ where F is a regular polygon any two reflections x and y in adjacent axes of symmetry satisfy $xy \neq yx$. Also, for any $n \geq 4$, the permutations $(1\ 2\ 3)$ and $(2\ 3\ 4)$ are elements of both S_n and A_n, and $(1\ 2\ 3)(2\ 3\ 4) = (1\ 2)(3\ 4)$ whereas $(2\ 3\ 4)(1\ 2\ 3) = (1\ 3)(2\ 4)$. The group S_3 is isomorphic to $S(\triangle)$ and is therefore non-abelian.

Each dihedral group $S(F)$ where F is a regular polygon is not simple, because its subgroup $S^+(F)$ of direct symmetries has index 2 in $S(F)$ and is therefore normal in $S(F)$. Similarly, each symmetric group S_n with $n \geq 3$ is not simple, because its subgroup A_n has index 2 in S_n and is therefore normal in S_n (as stated in Corollary E12 in Unit E1).

The first non-abelian alternating group, A_4, is not simple either, because, as you saw in Exercise E47 in Section 5 of Unit E1, its subgroup

$$K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

is a normal subgroup. However, the next alternating group, A_5, *is* simple, as is shown in the solution to Exercise E88 in Subsection 3.3 later in this unit.

In fact it can be shown that the alternating group A_5, which has order 60, is the *smallest* non-abelian simple group, and that in general the following theorem holds. This theorem was originally proved by Évariste Galois (see the blue box below).

Theorem E19

The alternating group A_n is simple for $n \geq 5$.

It turns out that answering the question 'Which finite non-abelian groups are simple?' is a vastly difficult task. You can read a little about its history in the boxes below.

Simple groups and polynomial equations

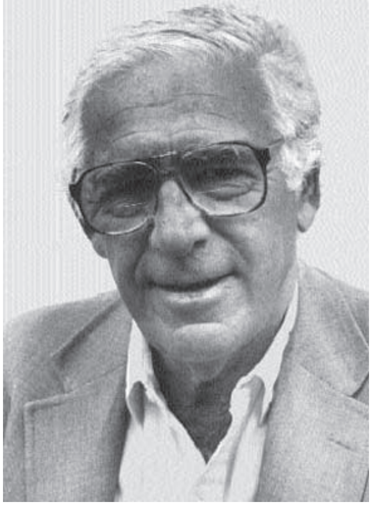
In 1799 the Italian mathematician Paolo Ruffini (1765–1822), building on earlier work of Lagrange on permutations, asserted and almost proved that the general quintic equation cannot be solved by radicals (in other words, there is no formula in terms of roots for the solutions of a polynomial equation of degree 5). The proof was completed by Niels Henrik Abel (1802–1829), who published it in 1824, with a longer, more detailed version in 1826.

Abel gave no criterion for distinguishing between polynomial equations that can be solved by radicals (such as $(x-1)^5 = 0$) and those that cannot. This issue was resolved by Évariste Galois (1811–1832), in a memoir written in 1830 when he was still a teenager but only published posthumously in 1846 (he died at the age of 20 following a duel). Galois showed that whether or not a polynomial equation is solvable by radicals is equivalent to whether or not a particular permutation group formed by its solutions has a certain structure. Fundamental for his resolution of the problem was his proof of the result that, in modern language, the alternating group A_n is simple for $n \geq 5$.

Galois' work was notoriously difficult for his contemporaries to understand and it took many decades before it was recast in the form in which it is studied today. For example, the term 'alternating group' was not used until 1873, when it appeared in an article by Camille Jordan.

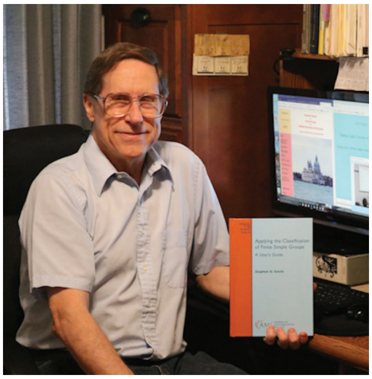
Niels Henrik Abel

Évariste Galois



Daniel Gorenstein

Michael Aschbacher



Stephen Smith

The classification of finite simple groups

Given the importance of finite simple groups – they can be thought of as the building blocks of all finite groups – it was natural for mathematicians to want to classify them. This led to a monumental collective effort that began in the nineteenth century and gathered pace in the second half of the twentieth century. About a hundred mathematicians were involved, and together they published several hundred journal articles covering tens of thousands of pages. Much of the work was overseen by Daniel Gorenstein (1923–1982) who said in 1979 that 'it makes more sense to view this classification as an entire field of mathematics rather than as an attempt to prove a single theorem'. Gorenstein announced in February 1981 that the classification was complete, but in fact the final gap in the proof was closed in 2004 by Michael Aschbacher (1944–) and Stephen Smith (1948–). The resulting theorem, one of the most extraordinary in pure mathematics, can be summarised as follows.

Classification theorem for finite simple groups

Let G be a finite simple group. Then G lies in one (or more) of the following families:

- the cyclic groups of prime order
- the alternating groups of degree at least 5
- the finite groups of Lie type (these groups are beyond the scope of this module)
- 26 groups known as the *sporadic groups*.

So apart from the 26 sporadic groups, all finite simple groups fit into patterns. The largest sporadic group is known as the *Monster*: it has order

$$2^{46} \times 3^{20} \times 5^{9} \times 7^{6} \times 11^{2} \times 13^{3} \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71,$$

which is approximately equal to 8×10^{53}.

The classification theorem is an enormously powerful result: many problems in group theory can be reduced to problems about simple groups or groups closely related to simple groups, allowing knowledge about simple groups to be used to solve them. By 2004 almost none of the major problems in finite group theory that were unsolved before 1980 remained open. However, the classification theorem has not ended research into finite groups, in much the same way that the discovery of the periodic table did not stop research in chemistry.

(Source: Gorenstein, D. (1979) 'The classification of finite simple groups 1. Simple groups and local analysis', *Bulletin of the American Mathematical Society* vol. 1, no. 1, pp. 43–199.)

2 Conjugacy

In this section you will start by revising the idea of *conjugacy* in symmetric groups, which you studied in Unit B3. Then you will see how this idea can be generalised to all groups. The idea of conjugacy is related to the existence of normal subgroups, and hence to the ability to construct quotient groups, as you will see in Section 3.

2.1 Conjugacy in symmetric groups

Remember that for each positive integer n the symmetric group S_n is the group of all permutations of the set $\{1, 2, \ldots, n\}$.

You met the following definition in Subsection 4.1 of Unit B3.

Definition

Let x and y be permutations in S_n. We say that y is a **conjugate** of x in S_n if there is a permutation g in S_n such that

$$y = g \circ x \circ g^{-1}.$$

We also say that:

- g **conjugates** x to y
- y is the **conjugate** of x by g
- g is a **conjugating permutation**.

For example, the permutation $(2\ 3\ 5)(4\ 6)$ is a conjugate of the permutation $(1\ 4\ 3)(2\ 6)$ in S_6 because $(1\ 3\ 2\ 4\ 5) \in S_6$ and

$$(2\ 3\ 5)(4\ 6) = (1\ 3\ 2\ 4\ 5) \circ (1\ 4\ 3)(2\ 6) \circ (1\ 3\ 2\ 4\ 5)^{-1}, \qquad (3)$$

as we will check shortly. This equation shows that $(1\ 3\ 2\ 4\ 5)$ conjugates $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$.

To check equation (3), we have to simplify the expression on the right-hand side. That is, we have to find the conjugate of $(1\ 4\ 3)(2\ 6)$ by $(1\ 3\ 2\ 4\ 5)$. One way to do this is to find the inverse of the permutation $(1\ 3\ 2\ 4\ 5)$, then compose the three permutations in the usual way. However, there is a much quicker way to find conjugates in a symmetric group, as follows.

Strategy E4 Renaming method

To find the conjugate $g \circ x \circ g^{-1}$, where x and g are permutations in S_n, replace each symbol in the cycle form of x by its image under g.

We refer to this strategy as the 'renaming method' because it involves 'renaming' each symbol in a permutation x using the conjugating permutation g. The reason why it works is explained shortly, but first here is a worked exercise to demonstrate it, and an exercise in which you can practise it.

Worked Exercise E24

Use the renaming method, Strategy E4, to find the conjugate

$$(1\ 3\ 2\ 4\ 5) \circ (1\ 4\ 3)(2\ 6) \circ (1\ 3\ 2\ 4\ 5)^{-1}.$$

Solution

Rename the symbols in (1 4 3)(2 6) using (1 3 2 4 5): that is, replace each symbol in (1 4 3)(2 6) by its image under (1 3 2 4 5).

We have

$$\begin{array}{rl} & (1\ 4\ 3)(2\ 6) \\ (1\ 3\ 2\ 4\ 5) & \ \downarrow\downarrow\downarrow\ \ \downarrow\downarrow \\ & (3\ 5\ 2)(4\ 6) = (2\ 3\ 5)(4\ 6). \end{array}$$

Thus

$$(1\ 3\ 2\ 4\ 5) \circ (1\ 4\ 3)(2\ 6) \circ (1\ 3\ 2\ 4\ 5)^{-1} = (2\ 3\ 5)(4\ 6).$$

Worked Exercise E24 confirms that (1 3 2 4 5) conjugates (1 4 3)(2 6) to (2 3 5)(4 6), as claimed by equation (3).

Exercise E68

(a) Use the renaming method, Strategy E4, to find the following conjugates in S_5.

(i) $(1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (1\ 3\ 5)^{-1}$

(ii) $(1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ \big((1\ 3)(2\ 4\ 5)\big)^{-1}$

(b) Check your answers to part (a) by finding the inverse of (1 3 5) and the inverse of (1 3)(2 4 5) and composing the permutations in the usual way.

To see why the renaming method, Strategy E4, works consider the example of the permutations

$$x = (1\ 4\ 3)(2\ 6) \quad \text{and} \quad g = (1\ 3\ 2\ 4\ 5)$$

in S_6, from Worked Exercise E24. Let y be the permutation obtained by renaming the symbols in x using g, as shown below.

$$\begin{array}{rl} & x = (1\ 4\ 3)(2\ 6) \\ (1\ 3\ 2\ 4\ 5) = g \downarrow & \quad\ \ \downarrow\downarrow\downarrow\ \ \downarrow\downarrow \\ & y = (3\ 5\ 2)(4\ 6) \end{array} \tag{4}$$

Strategy E4 claims that y is equal to $g \circ x \circ g^{-1}$. Here is an explanation of why this is.

Let us focus on one particular symbol in the set $\{1, 2, 3, 4, 5, 6\}$, say 3, and find its image under y. We can see immediately from the cycle form of y found above that the image of 3 under y is 5. Let us find the image of 3 under y in another way, namely by using the cycle form of x, since y is just x with the symbols renamed. We proceed as follows. We first find the symbol that was renamed as 3. To do this, we go backwards along the arrow that points to the symbol 3 in diagram (4) above. That is, we find the image of 3 under the permutation g^{-1}. This gives the symbol 1. Then we use the cycle form of x to find the image of 1 under x. This gives 4. Finally, we find the symbol that is the new name of the symbol 4. That is, we find the image of 4 under the permutation g. This gives 5. So we have found in another way that the image of 3 under y is 5.

The process described above shows that the effect of applying the permutation y to the symbol 3 is the same as the effect of applying the permutation g^{-1}, then the permutation x, then the permutation g to the symbol 3, as illustrated in Figure 11. That is, the two permutations y and $g \circ x \circ g^{-1}$ have the same effect on the symbol 3. There is nothing special about the symbol 3 here, of course: the same will be true for any symbol in the set $\{1, 2, 3, 4, 5, 6\}$. In other words, the permutations y and $g \circ x \circ g^{-1}$ are equal, as claimed.

$$\begin{tikzcd}
1 \arrow[r, "x"] & 4 \arrow[d, "g"] \\
3 \arrow[u, "g^{-1}"] \arrow[r, "y"'] & 5
\end{tikzcd}$$

Figure 11 The image of the symbol 3 under the permutation y, found in two different ways

The ideas above hold whenever we use a permutation g to rename the symbols in a permutation x: the permutation that we obtain is equal to $g \circ x \circ g^{-1}$. This explains why Strategy E4 works.

Notice that the equation

$$y = g \circ x \circ g^{-1}$$

in the definition of a conjugate can be rearranged as

$$g^{-1} \circ y \circ g = x$$

(by composing both sides of the original equation on the left by g^{-1} and on the right by g). The rearranged equation can be written as

$$x = g^{-1} \circ y \circ (g^{-1})^{-1}.$$

Thus if g conjugates x to y, then g^{-1} conjugates y to x. This makes sense in view of Strategy E4, because if renaming the symbols in x using g gives y, then of course renaming the symbols in y using g^{-1} gives x.

So if y is a conjugate of x in S_n, then x is a conjugate of y in S_n, and we can simply say that x and y are **conjugates** or **conjugate permutations** in S_n, or that they are **conjugate** in S_n. These are all ways of saying that each of x and y is a conjugate of the other in S_n.

Since renaming the symbols in a permutation does not change its cycle structure, permutations that are conjugate in S_n always have the same cycle structure.

It is also true that any two permutations in S_n with the same cycle structure are conjugate in S_n. This is because if two permutations x and y in S_n have the same cycle structure, then there is always at least one permutation g in S_n that conjugates x to y; it can be found by using the following strategy, which you met in Unit B3.

Strategy B12

To find a permutation g such that $y = g \circ x \circ g^{-1}$, where x and y are permutations with the same cycle structure, do the following.

Use the fact that g renames x to y, as follows.

1. Match up the cycles of x and y (including 1-cycles) so that cycles of equal lengths correspond.

$$\begin{array}{rl} x = & (* \;\; * \;\; \cdots \;\; *)(* \;\; * \;\; \cdots \;\; *)\cdots(*)(*) \\ g \downarrow & \;\;\downarrow \;\; \downarrow \;\; \cdots \;\; \downarrow \;\;\; \downarrow \;\; \downarrow \;\; \cdots \;\; \downarrow \;\; \cdots \;\; \downarrow \;\; \downarrow \\ y = & (* \;\; * \;\; \cdots \;\; *)(* \;\; * \;\; \cdots \;\; *)\cdots(*)(*) \end{array}$$

2. Read off the two-line form of the renaming permutation g from this diagram. Usually, write g in cycle form.

Worked Exercise E25

(a) Use Strategy B12 to find a permutation g in S_6 that conjugates $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$.

(b) Find another permutation g in S_6 that does this.

Solution

(a) Write the cycle form of $(2\ 3\ 5)(4\ 6)$ underneath the cycle form of $(1\ 4\ 3)(2\ 6)$, matching up cycles of the same length, and including the 1-cycles.

We can write

$$\begin{array}{rl} & (1\ \ 4\ \ 3)(2\ \ 6)(5) \\ g & \;\downarrow\,\downarrow\,\downarrow\;\;\downarrow\,\downarrow\;\;\downarrow \\ & (2\ \ 3\ \ 5)(4\ \ 6)(1). \end{array}$$

Interpret this diagram as the two-line form of a conjugating permutation g, and write down the cycle form of g. The permutation g maps 1 to 2, so it has a cycle starting $(1\ 2\ \cdots)$. It maps 2 to 4, so the cycle continues $(1\ 2\ 4\ \cdots)$. We continue in this way to find the cycle form of g.

A conjugating permutation g is

$$g = (1\ 2\ 4\ 3\ 5)(6) = (1\ 2\ 4\ 3\ 5).$$

(b) There are several alternative ways to match up the cycles in the permutations (2 3 5)(4 6) and (1 4 3)(2 6), because the starting numbers in the cycles can be changed.

Another conjugating permutation g is given by

$$\begin{array}{rl} & (1\ 4\ 3)(2\ 6)(5) \\ g & \ \downarrow\,\downarrow\,\downarrow\quad\downarrow\,\downarrow\quad\downarrow \\ & (5\ 2\ 3)(4\ 6)(1). \end{array}$$

This gives

$$g = (1\ 5)(3)(2\ 4)(6) = (1\ 5)(2\ 4).$$

Exercise E69

There are six permutations in S_6 that conjugate (1 4 3)(2 6) to (2 3 5)(4 6). One of these, (1 3 2 4 5), was given in Worked Exercise E24, and another two, (1 2 4 3 5) and (1 5)(2 4), were found in Worked Exercise E25. Determine the other three permutations.

Exercise E70

Find all the permutations in S_4 that conjugate (1 3) to (3 4).

The discussion in this subsection justifies the following theorem, which you met in Unit B3.

Theorem B64

Two permutations in the symmetric group S_n are conjugate in S_n if and only if they have the same cycle structure.

Since the order of a permutation depends only on its cycle structure, it follows from Theorem B64 that permutations that are conjugate in S_n always have the same order.

2.2 Conjugacy in general

So far you have seen the idea of conjugacy applied only to symmetric groups. We will now extend the idea of conjugacy to all groups. We make the following definition.

Definition

Let x and y be elements of a group G. We say that y is a **conjugate** of x in G if there exists an element g in G such that

$$y = gxg^{-1}.$$

We also say that

- g **conjugates** x to y
- y is the **conjugate** of x by g
- g is a **conjugating element**.

This definition is written using concise multiplicative notation for a general group G, in the usual way. If the binary operation of a particular group G is denoted by $\circ$, for example, then as you would expect we write a conjugate in G in the form $g \circ x \circ g^{-1}$ rather than gxg^{-1}. For example, this applies to symmetric groups and symmetry groups.

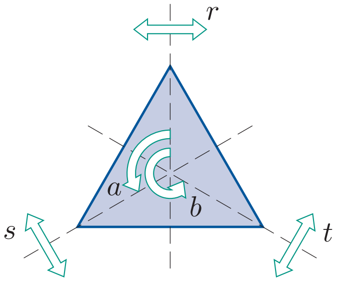


Figure 12 The symmetries of the equilateral triangle

Table 5 $S(\triangle)$

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

Worked Exercise E26

Find the conjugate $r \circ a \circ r^{-1}$ in the group $S(\triangle)$.

(The non-identity symmetries of the equilateral triangle are shown in Figure 12 and the group table of $S(\triangle)$ is given as Table 5.)

Solution

$r \circ a \circ r^{-1} = r \circ a \circ r = r \circ (a \circ r) = r \circ t = b$

Exercise E71

Find the following conjugates in the group $S(\triangle)$.

(a) $s \circ a \circ s^{-1}$ (b) $a \circ a \circ a^{-1}$ (c) $e \circ a \circ e^{-1}$ (d) $b \circ a \circ b^{-1}$

Exercise E72

Let G be an abelian group and let $x \in G$. Show that for all $g \in G$ the conjugate of x by g is equal to x.

Exercise E72 shows that in an abelian group the only conjugate of an element x is x itself. So conjugacy in an abelian group is rather boring! In a non-abelian group, a conjugate of an element x may be x itself or it may be a different element, as illustrated by Worked Exercise E26 and Exercise E71 above.

Exercise E73

Let G be a group with identity e and let $x \in G$.

(a) Show that the conjugate of e by x is equal to e.

(b) Show that the conjugate of x by e is equal to x.

Exercise E73(a) shows that in any group the only conjugate of the identity element e is itself. Exercise E73(b) shows that in any group every element is a conjugate of itself.

In the previous subsection you saw that, in a symmetric group S_n, if a permutation y is a conjugate of a permutation x, then x is also a conjugate of y. This property extends to conjugates in any group: if y is a conjugate of x in the group, then x is also a conjugate of y in the group. The justification of this is the same as for conjugates in S_n: the equation

$$y = gxg^{-1}$$

in the definition of a conjugate can be rearranged as

$$g^{-1}yg = x$$

(by composing both sides of the original equation on the left by g^{-1} and on the right by g), and the rearranged equation can be written as

$$x = g^{-1}y(g^{-1})^{-1}.$$

This shows that if g conjugates x to y, then g^{-1} conjugates y to x. Because of this, instead of saying that y is a conjugate of x in a group G, we can simply say that x and y are **conjugates** or **conjugate elements** in G, or that they are **conjugate** in G. These are all ways of saying that each of x and y is a conjugate of the other in G.

There is another useful property of conjugacy in symmetric groups that extends to any group. You saw in the previous subsection that conjugate permutations have the same cycle structure, and therefore have the same order. In fact, conjugate elements have the same order in any group.

To help us prove this result, we will first prove a lemma. In the next exercise you are asked to confirm some particular cases of this lemma, and then the lemma is stated with a general proof.

Exercise E74

Let x, y and g be elements of a group, and suppose that $y = gxg^{-1}$. Prove each of the following.

(a) $y^2 = gx^2g^{-1}$ (b) $y^3 = gx^3g^{-1}$ (c) $y^4 = gx^4g^{-1}$

From the solution to Exercise E74 it is apparent that the pattern in the exercise will continue for all positive integers n. In other words, the lemma below holds. To prove this result formally, we use mathematical induction, which you met in Unit A3 *Mathematical language and proof*.

Lemma E20

Let x, y and g be elements of a group, and suppose that $y = gxg^{-1}$. Then $y^n = gx^ng^{-1}$ for all positive integers n.

Proof We use mathematical induction. Let $P(n)$ be the statement

$$y^n = gx^ng^{-1}.$$

Then $P(1)$ is $y = gxg^{-1}$, which is true.

We now need to show that $P(k) \implies P(k+1)$ for each positive integer k.

Now let k be a positive integer and assume that $P(k)$ is true; that is,

$$y^k = gx^kg^{-1}.$$

We need to prove under this assumption that $P(k+1)$ is true, that is,

$$y^{k+1} = gx^{k+1}g^{-1}.$$

Now

$$\begin{aligned} y^{k+1} &= y^ky \\ &= gx^kg^{-1}gxg^{-1} \quad (\text{by } P(k) \text{ and since } y = gxg^{-1}) \\ &= gx^kexg^{-1} \\ &= gx^{k+1}g^{-1}. \end{aligned}$$

Thus $P(k+1)$ is true. So we have shown that

$$P(k) \implies P(k+1) \quad \text{for each positive integer } k.$$

Hence, by mathematical induction, it follows that $P(n)$ is true for all positive integers n. That is, $y^n = gx^ng^{-1}$ for all positive integers n. ■

We can now prove the result below. Remember that the order of a group element x is the *smallest* positive integer n such that $x^n = e$, if there is such an integer n. If there is no such integer n, then x has infinite order.

Theorem E21

Let x and y be conjugate elements in a group G. Then either x and y have the same finite order, or they both have infinite order.

Proof Since x and y are conjugate elements, there exists an element g in G such that $y = gxg^{-1}$. It follows that $x = g^{-1}yg$.

We now show that for any positive integer n,

$$x^n = e \quad \text{if and only if} \quad y^n = e. \tag{5}$$

To do this, let n be a positive integer, and first suppose that $x^n = e$. Then

$$\begin{aligned} y^n &= gx^n g^{-1} \quad \text{(by Lemma E20, since } y = gxg^{-1}\text{)} \\ &= geg^{-1} \\ &= e. \end{aligned}$$

Now suppose instead that $y^n = e$. Then

$$\begin{aligned} x^n &= g^{-1}y^n g \quad \text{(by Lemma E20, since } x = g^{-1}yg; \\ &\qquad\qquad \text{here } g^{-1} \text{ is the conjugating element)} \\ &= g^{-1}eg \\ &= e. \end{aligned}$$

We have now shown that statement (5) holds. This statement tells us that the positive integers n for which $x^n = e$ are exactly the same as the positive integers n for which $y^n = e$. It follows that either x and y have the same finite order, or both have infinite order. ■

The converse of Theorem E21 is not true: that is, group elements of the same order are not necessarily conjugate. For example, in the symmetric group S_4 the permutations $(1\ 2)$ and $(1\ 2)(3\ 4)$ both have order 2, but they are not conjugate because they have different cycle structures.

Exercise E75

Find two elements in the group $\mathbb{Z}_6$ that have the same order but are not conjugate in $\mathbb{Z}_6$.

2.3 Conjugacy classes

We now consider the set of all elements in a group that are conjugate to a particular element. We make the following definition.

Definition

Let G be a group, and let $x \in G$. The **conjugacy class** of x in G is the set of all elements of G that are conjugate to x. That is, it is the set

$$\{gxg^{-1} : g \in G\}.$$

Worked Exercise E27

Find the conjugacy class of the element a in $S(\square)$.

(The group table of $S(\square)$ is given as Table 6.)

Table 6 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

Solution

We find all the conjugates of a in $S(\square)$.

The conjugates of a in $S(\square)$ are

$$\begin{aligned}
e \circ a \circ e^{-1} &= e \circ (a \circ e) = e \circ a = a,\\
a \circ a \circ a^{-1} &= a \circ e = a,\\
b \circ a \circ b^{-1} &= b \circ (a \circ b) = b \circ c = a,\\
c \circ a \circ c^{-1} &= c \circ (a \circ a) = c \circ b = a,\\
r \circ a \circ r^{-1} &= r \circ (a \circ r) = r \circ s = c,\\
s \circ a \circ s^{-1} &= s \circ (a \circ s) = s \circ t = c,\\
t \circ a \circ t^{-1} &= t \circ (a \circ t) = t \circ u = c,\\
u \circ a \circ u^{-1} &= u \circ (a \circ u) = u \circ r = c.
\end{aligned}$$

There are only two distinct conjugates: a and c.

So the conjugacy class of a in $S(\square)$ is $\{a, c\}$.

Exercise E76

Find the conjugacy class of each of the following elements in $S(\square)$.

(a) c (b) e

A group element is always an element of its own conjugacy class, as illustrated by the solutions to Worked Exercise E27 and Exercise E76. This is because conjugating a group element x by the identity element e always gives x again: $exe^{-1} = x$.

If we extend the calculations in Worked Exercise E27 and Exercise E76 to find the conjugacy class of every element of $S(\square)$, then we obtain the following.

Element	Conjugacy class
e	$\{e\}$
a	$\{a, c\}$
b	$\{b\}$
c	$\{a, c\}$
r	$\{r, t\}$
s	$\{s, u\}$
t	$\{r, t\}$
u	$\{s, u\}$

Notice that some of the conjugacy classes here are the same; in fact, there are only five *distinct* conjugacy classes, as follows:

$$\{e\}, \quad \{b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

Notice also that there is no overlap between any two of the distinct conjugacy classes: the conjugacy classes of any two elements in $S(\square)$ are either exactly the same set or disjoint sets. Thus the distinct conjugacy classes of the elements of $S(\square)$ form a *partition* of $S(\square)$, as shown in Figure 13. That is, they split $S(\square)$ into a family of subsets whose union is the whole group, and each pair of which are disjoint.

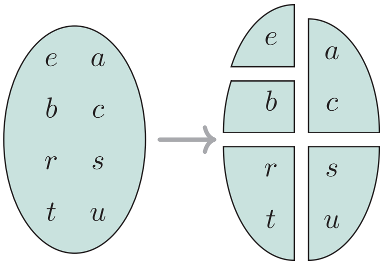


Figure 13 The partition of $S(\square)$ into conjugacy classes

In fact, like the left (or right) cosets of a subgroup, the distinct conjugacy classes of the elements of any group form a partition of the group.

This is because, as proved below, the relation 'is a conjugate of', defined on any group, is an *equivalence relation*, and the conjugacy classes are its equivalence classes. (You met equivalence relations in Unit A3.) In fact, you have already seen that the relation 'is a conjugate of' on any group has the *reflexive property*: you saw that each element x is a conjugate of itself. You have also seen that it has the *symmetric property*: you saw that if y is a conjugate of x, then x is a conjugate of y. The third property that has to be satisfied for a relation to be an equivalence relation is the *transitive property*. The proof below reminds you of its definition, and includes proofs of all three properties, for completeness.

Theorem E22

Let G be a group. Then the relation 'is a conjugate of' is an equivalence relation on the set of elements of G.

Proof We show that the relation 'is a conjugate of' defined on G is reflexive, symmetric and transitive.

E1 Reflexive property

We have to show that for all $x \in G$, x is a conjugate of x.

Let $x \in G$. Then $x = exe^{-1}$, so x is a conjugate of x. Thus the relation is reflexive.

E2 Symmetric property

We have to show that for all $x, y \in G$, if x is a conjugate of y then y is a conjugate of x.

Let $x, y \in G$, and suppose that x is a conjugate of y. Then there is an element $g \in G$ such that

$$x = gyg^{-1}.$$

Composing both sides of this equation on the left by g^{-1} and on the right by g, we obtain

$$g^{-1}xg = y,$$

and this equation can be written as

$$y = g^{-1}x(g^{-1})^{-1}.$$

Thus g^{-1} conjugates x to y, so y is a conjugate of x. Thus the relation is symmetric.

E3 Transitive property

We have to show that for all $x, y, z \in G$, if x is a conjugate of y and y is a conjugate of z then x is a conjugate of z.

Let $x, y, z \in G$, and suppose that x is a conjugate of y and y is a conjugate of z. Then there are elements g_1 and g_2 in G such that

$$x = g_1yg_1^{-1} \quad \text{and} \quad y = g_2zg_2^{-1}.$$

Using the second equation to substitute for y in the first equation gives

$$x = g_1g_2zg_2^{-1}g_1^{-1},$$

which (by Proposition B14 in Unit B1) we can write as

$$x = g_1g_2z(g_1g_2)^{-1}.$$

Thus g_1g_2 conjugates z to x, so x is a conjugate of z. Thus the relation is transitive.

Hence the relation 'is a conjugate of' is an equivalence relation on G. ■

From Theorem E22 we can deduce the following, illustrated in Figure 14.

Corollary E23

In any group, the distinct conjugacy classes form a partition of the group.

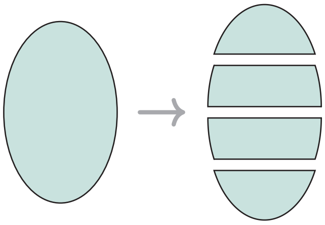


Figure 14 The partition of a group into conjugacy classes

Proof The conjugacy class of an element x of a group G is the set of all elements of G that are conjugate to x. In other words, it is the equivalence class of x with respect to the equivalence relation 'is a conjugate of' defined on G. So the distinct conjugacy classes are the distinct equivalence classes of this equivalence relation, and hence they partition G. ■

We refer to the distinct conjugacy classes of the elements of a group G as the **conjugacy classes of** G. For example, you saw after Exercise E76 that the conjugacy classes of $S(\square)$ are

$$\{e\}, \quad \{b\}, \quad \{a,c\}, \quad \{r,t\}, \quad \{s,u\}.$$

Every group has at least one conjugacy class that is quick to find. As you saw in Exercise E73(a), conjugating the identity element e of a group by any other element g just gives the identity element again: $geg^{-1} = gg^{-1} = e$. So the following holds.

Proposition E24

Let G be a group with identity element e. Then $\{e\}$ is a conjugacy class of G.

For a *finite* group G, we can find all the other conjugacy classes of G by working out the conjugacy class of each element, in the way demonstrated in Worked Exercise E27 and Exercise E76, and then assembling all the distinct conjugacy classes.

A much more efficient method, which applies because the conjugacy classes partition the group, is to use a strategy similar to the one that we used for cosets of a subgroup: we repeatedly choose an element not yet assigned to a conjugacy class and find its conjugacy class, until all the elements have been assigned to conjugacy classes.

However, there are usually still more efficient ways to proceed. For example, we can sometimes cut down the work by using the fact that conjugate elements always have the same order, by Theorem E21.

To illustrate this, let us use this approach to confirm that the conjugacy classes of $S(\square)$ are as listed above. The non-identity elements of $S(\square)$ are shown in Figure 15. We know that elements of different orders cannot be conjugate, so to partition $S(\square)$ into conjugacy classes we can start by partitioning it according to the orders of its elements. The identity element has order 1, the elements a and c both have order 4, and the elements b, r, s, t and u all have order 2, so the partition of $S(\square)$ by the orders of its elements is

$$\{e\}, \quad \{a, c\}, \quad \{b, r, s, t, u\}.$$

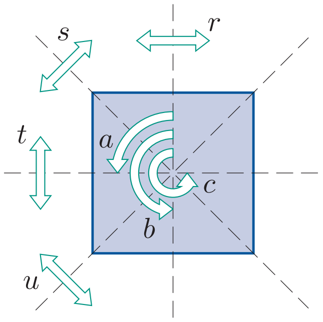


Figure 15 $S(\square)$

We know that each conjugacy class of $S(\square)$ is either one of these three sets or is obtained by splitting one of these sets into two or more conjugacy classes.

To determine whether the set $\{a, c\}$, for example, is a conjugacy class or whether it splits further, we can start conjugating the element a by each element of $S(\square)$ in turn. If we find a conjugate that is equal to c, then this tells us that $\{a, c\}$ is a conjugacy class, and there is no need to find any more conjugates. On the other hand, if after conjugating a by all the elements of $S(\square)$ we have found that no conjugate of a is equal to c, then this tells us that the set $\{a, c\}$ must split into the two conjugacy classes $\{a\}$ and $\{c\}$. We can carry out a similar process for the set $\{b, r, s, t, u\}$.

This method is demonstrated in the worked exercise below.

Worked Exercise E28

Find the conjugacy classes of the group $S(\square)$.

(The group table of $S(\square)$ is given as Table 7.)

Table 7 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

Solution

Start by partitioning $S(\square)$ by the orders of its elements.

The partition of $S(\square)$ by the orders of its elements is

$$\{e\}, \quad \{a, c\}, \quad \{b, r, s, t, u\}.$$

Hence the set $\{e\}$ is a conjugacy class.

Consider the set $\{a, c\}$.

We find conjugates of a to see if we can obtain c. There is no point in conjugating a by any of the elements e, a, b or c, as that will give a again, since $\{e, a, b, c\}$ is an abelian subgroup of $S(\square)$. Let us try conjugating a by r.

We have

$$r \circ a \circ r^{-1} = r \circ (a \circ r) = r \circ s = c.$$

Hence $\{a, c\}$ is a conjugacy class.

Now consider the set $\{b, r, s, t, u\}$.

We find conjugates of b to see if we can obtain any of r, s, t and u.

Conjugating b by any of e, a, b or c will give b again, since $\{e, a, b, c\}$ is an abelian subgroup of $S(\square)$. Also,

$$\begin{aligned}
r \circ b \circ r^{-1} &= r \circ (b \circ r) = r \circ t = b,\\
s \circ b \circ s^{-1} &= s \circ (b \circ s) = s \circ u = b,\\
t \circ b \circ t^{-1} &= t \circ (b \circ t) = t \circ r = b,\\
u \circ b \circ u^{-1} &= u \circ (b \circ u) = u \circ s = b.
\end{aligned}$$

Hence $\{b\}$ is a conjugacy class.

Now we find conjugates of r to see if we can obtain any of s, t and u.

Conjugating r by e or r will give r. Also,

$$\begin{aligned}
a \circ r \circ a^{-1} &= a \circ (r \circ c) = a \circ s = t,\\
b \circ r \circ b^{-1} &= b \circ (r \circ b) = b \circ t = r,\\
c \circ r \circ c^{-1} &= c \circ (r \circ a) = c \circ u = t,\\
s \circ r \circ s^{-1} &= s \circ (r \circ s) = s \circ c = t,\\
t \circ r \circ t^{-1} &= t \circ (r \circ t) = t \circ b = r,\\
u \circ r \circ u^{-1} &= u \circ (r \circ u) = u \circ a = t.
\end{aligned}$$

Hence $\{r, t\}$ is a conjugacy class.

Now we just need to find conjugates of s to see if we can obtain u. We know that conjugating s by e or s will give s again. Let us try conjugating s by a.

Finally, we have

$$a \circ s \circ a^{-1} = a \circ (s \circ c) = a \circ t = u.$$

Hence $\{s, u\}$ is a conjugacy class.

In summary, the conjugacy classes of $S(\square)$ are

$$\{e\}, \quad \{a, c\}, \quad \{b\}, \quad \{r, t\}, \quad \{s, u\}.$$

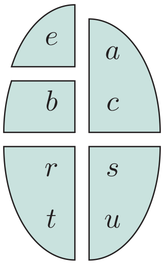


Figure 16 The conjugacy classes of $S(\square)$

The partition of $S(\square)$ into conjugacy classes is shown in Figure 16.

Exercise E77

Find the conjugacy classes of the group $S(\triangle)$.

(The non-identity elements of $S(\triangle)$ are shown in Figure 17, and the group table of $S(\triangle)$ is given as Table 8.)

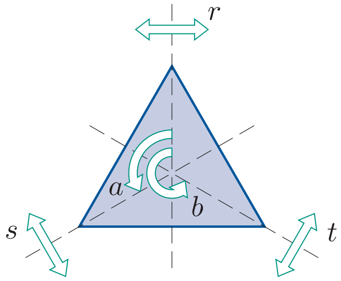


Figure 17 The symmetries of the equilateral triangle

Table 8 $S(\triangle)$

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

For *symmetry groups*, such as $S(\square)$ and $S(\triangle)$, there are in fact very efficient ways to find the conjugacy classes, as you will see in Section 4.

Exercise E78

Partition the group $\mathbb{Z}_7^*$ into its conjugacy classes.

Hint: Use the result proved in Exercise E72 in Subsection 2.2.

Exercise E78 illustrates the following result (it is just the result proved in the solution to Exercise E72 restated in terms of conjugacy classes).

Theorem E25

In an abelian group, each conjugacy class contains a single element.

Proof Let G be an abelian group and let x be any element of G. Since G is abelian, for any element $g \in G$ we have

$$gxg^{-1} = gg^{-1}x = ex = x.$$

So the only conjugate of x is x itself. Hence the conjugacy class of x is $\{x\}$. ■

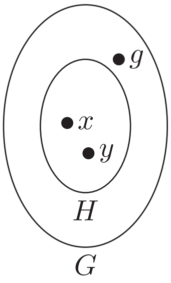


Figure 18 Elements x, y and g in a group G with a subgroup H

Whenever you work with conjugates, you need to be aware of the following important but quite subtle point. When we say that *elements x and y are conjugate in the group G*, the 'in the group G' part is crucial. This is because if H is a subgroup of a group G and x and y are elements of H, as illustrated in Figure 18, then it is possible for x and y to be conjugate in G but not conjugate in H. The reason for this is that if x and y are conjugate in G, then although we know that there is an element g in G such that $y = gxg^{-1}$, as also illustrated in Figure 18, there may not be any such element g in the subgroup H.

For example, consider the group $S(\square)$. As you saw in Subsection 2.4 of Unit B3, we can represent this group as a subgroup of the symmetric group S_4 by representing its elements as permutations of vertex labels (see Figure 19), as follows.

e	$r = (1\ 4)(2\ 3)$
$a = (1\ 2\ 3\ 4)$	$s = (2\ 4)$
$b = (1\ 3)(2\ 4)$	$t = (1\ 2)(3\ 4)$
$c = (1\ 4\ 3\ 2)$	$u = (1\ 3)$

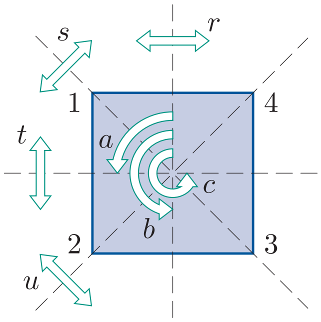


Figure 19 $S(\square)$

The conjugacy classes of $S(\square)$, found in Worked Exercise E28, are

$$\{e\}, \quad \{b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

With the elements of $S(\square)$ represented as permutations as above, these conjugacy classes are

$$\{e\},\quad \{(1\ 3)(2\ 4)\},\quad \{(1\ 2\ 3\ 4),\ (1\ 4\ 3\ 2)\},$$
$$\{(1\ 4)(2\ 3),\ (1\ 2)(3\ 4)\},\quad \{(2\ 4),\ (1\ 3)\}.$$

So the elements $b = (1\ 3)(2\ 4)$ and $r = (1\ 4)(2\ 3)$, for example, are *not* conjugate in $S(\square)$. However, they *are* conjugate in the group S_4 because they have the same cycle structure. So although there is an element g in S_4 that conjugates $b = (1\ 3)(2\ 4)$ to $r = (1\ 4)(2\ 3)$, there is no such element g in the subgroup $S(\square)$ of S_4.

Now consider again the general situation where a group H is a subgroup of a group G and x and y are elements of H, as illustrated in Figure 18 above. You have seen that if x and y are conjugate in G, then they are not necessarily conjugate in H. However, if x and y *are* conjugate in H, then they are also conjugate in G. This is because if x and y are conjugate in H, then there is an element h of H such that $y = hxh^{-1}$, as illustrated in Figure 20, and since $h \in G$ this equation shows that x and y are conjugate in G.

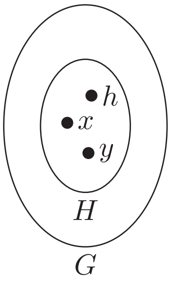


Figure 20 Elements x, y and h in a subgroup H of a group G

The discussion above proves the following proposition.

Proposition E26

Let H be a subgroup of a group G, and let x and y be elements of H.

(a) If x and y are conjugate in H, then they are also conjugate in G.

(b) If x and y are conjugate in G, then they may or may not be conjugate in H.

The contrapositive of Proposition E26(a) is:

> If x and y are not conjugate in G, then they are not conjugate in H.

This fact will be useful later in the unit.

Exercise E79

Consider the subgroup

$$H = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

of the group S_4 (this subgroup represents the symmetry group of the rectangle when its vertices are labelled in the usual way, as shown in Figure 21). Explain how you know that no two elements of H are conjugate to each other in H, but all the non-identity elements of H are conjugate to each other in S_4.

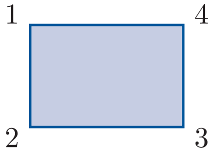


Figure 21 A labelled rectangle

Notice that the representation of the elements of $S(\square)$ as permutations,

$$\begin{array}{ll} e, & r = (1\ 4)(2\ 3), \\ a = (1\ 2\ 3\ 4), & s = (2\ 4), \\ b = (1\ 3)(2\ 4), & t = (1\ 2)(3\ 4), \\ c = (1\ 4\ 3\ 2), & u = (1\ 3), \end{array}$$

makes it clear that the elements r and t of $S(\square)$ do not lie in the same conjugacy class of $S(\square)$ as the elements s and u, as follows. The cycle structure $(-\ -)(-\ -)$ of r and t is different from the cycle structure $(-\ -)$ of s and u, so neither of r and t is conjugate to either of s and u in S_4, and hence the same must be true in the subgroup $S(\square)$ of S_4. We will use this idea, and others, to help us find conjugacy classes of symmetry groups in Section 4.

We end this subsection with a useful result about the conjugacy classes of finite groups.

To illustrate it, consider the conjugacy classes of the group $S(\square)$. You have seen that they are as follows:

$$\{e\}, \quad \{b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

The numbers of elements in these conjugacy classes are 1, 1, 2, 2 and 2, respectively, and each of these numbers divides 8, the order of $S(\square)$.

A similar fact is true for the conjugacy classes of the group $S(\triangle)$, which as you have seen are as follows:

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

The numbers of elements in these conjugacy classes are 1, 2 and 3, respectively, and each of these numbers divides 6, the order of $S(\triangle)$.

The following general result holds. It is proved in Unit E4.

Theorem E27

In any finite group G, the number of elements in each conjugacy class divides the order of G.

3 Normal subgroups and conjugacy

In Unit E1 you saw that a subgroup H of a group G is a **normal subgroup** of G if the partition of G into left cosets of H is the same as the partition of G into right cosets of H. You saw that this condition can be expressed algebraically as

$$gH = Hg \quad \text{for each element } g \in G.$$

In this section you will meet three conditions that are equivalent to this condition, and that we can therefore use as alternatives to check whether a subgroup is normal. These three conditions all involve conjugacy, and are often more convenient than the condition above.

We refer to checking whether a subgroup is normal or not as checking its **normality**.

3.1 Normal subgroups and conjugates

In this first subsection you will meet a condition for normality that involves conjugate elements.

To introduce it, let us suppose that we know that a particular subgroup H of a group G is a normal subgroup of G. Let h and g be any elements of H and G, respectively. Then, by the definition of a left coset,

$$gh \in gH.$$

Hence, since H is normal and so $gH = Hg$,

$$gh \in Hg.$$

Therefore

$$gh = h_1 g$$

for some element $h_1 \in H$. Composing both sides of this equation on the right by g^{-1} gives

$$ghg^{-1} = h_1.$$

Hence

$$ghg^{-1} \in H.$$

So we have found that, as illustrated in Figure 22,

> if H is a normal subgroup of a group G, then for any element h in H and any element g in G, the conjugate ghg^{-1} always lies in H.

In other words,

> if H is a normal subgroup of a group G, then conjugating any element of H by any element of G always gives an element of H.

It turns out that the converse of this statement is also true; that is,

> if conjugating any element of a subgroup H of a group G by any element of G always gives an element of H, then H is normal in G.

Hence we have the following theorem. It is proved fully in Subsection 3.4.

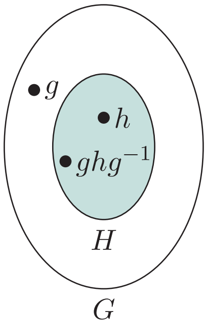


Figure 22 A normal subgroup H of a group G: conjugating any element of H by any element of G always gives an element of H

Theorem E28

Let G be a group and let H be a subgroup of G. Then H is a normal subgroup of G if and only if

$$ghg^{-1} \in H \quad \text{for each } h \in H \text{ and each } g \in G.$$

Theorem E28 gives us an alternative way to determine whether a subgroup is normal: we say that it **characterises** normal subgroups.

The characterisation of normal subgroups in Theorem E28 is more useful than our original definition of a normal subgroup for groups of large order or infinite order. To use it to prove that a subgroup H of a group G is normal in G, we take a general element $g \in G$ and a general element $h \in H$, and show that the conjugate ghg^{-1} belongs to H. As an illustration of this, here are alternative proofs of two results that you met in Unit E1.

Theorem E10

In an abelian group, every subgroup is normal.

Proof Let H be a subgroup of an abelian group G. We use Theorem E28 to show that H is normal in G. Let h be any element of H and let g be any element of G. We need to show that $ghg^{-1} \in H$.

We have

$$\begin{aligned} ghg^{-1} &= hgg^{-1} \quad \text{(since } G \text{ is abelian)} \\ &= he \\ &= h. \end{aligned}$$

Thus $ghg^{-1} \in H$. It follows that H is a normal subgroup of G. ■

Corollary E12

For each natural number n, the alternating group A_n is a normal subgroup of the symmetric group S_n.

Proof We use Theorem E28 to show that A_n is normal in S_n. Let h be any element of A_n and let g be any element of S_n. We have to show that $g \circ h \circ g^{-1} \in A_n$, that is, we have to show that $g \circ h \circ g^{-1}$ is an even permutation. We consider separately the possibilities that g is even and that g is odd.

If g is even, then g^{-1} is even and hence $g \circ h \circ g^{-1}$ is

$$\text{even} + \text{even} + \text{even} = \text{even}.$$

If g is odd, then g^{-1} is odd and hence $g \circ h \circ g^{-1}$ is

$$\text{odd} + \text{even} + \text{odd} = \text{even}.$$

Thus, in each case, $g \circ h \circ g^{-1} \in A_n$. It follows that A_n is a normal subgroup of S_n. ■

Here are some exercises in which you can practise using Theorem E28.

Exercise E80

Use Theorem E28 to provide an alternative proof of Theorem E9 in Unit E1. That is, prove that for any group G the trivial subgroup $\{e\}$ and the whole group G are normal subgroups of G.

Exercise E81

By Theorem B81 in Unit B4 *Lagrange's Theorem and small groups*, if H and K are subgroups of a group G, then so is $H \cap K$. Use this result and Theorem E28 to prove that if H and K are normal subgroups of a group G, then so is $H \cap K$.

Exercise E82

In Worked Exercise B18 in Subsection 1.2 of Unit B2 you met the group $(X, *)$ where X is the subset of $\mathbb{R}^2$ consisting of all the points not on the y-axis, that is,

$$X = \{(a, b) \in \mathbb{R}^2 : a \neq 0\},$$

and $*$ is the binary operation defined on X by

$$(a, b) * (c, d) = (ac, ad + b).$$

It was shown that in this group the identity element is $(1, 0)$ and the inverse of the element (a, b) is $\left(\frac{1}{a}, -\frac{b}{a}\right)$.

(a) As a reminder, verify the following in $(X, *)$.

(i) $(a, b) * (1, 0) = (a, b)$ for all $(a, b) \in X$.

(ii) $\left(\frac{1}{a}, -\frac{b}{a}\right) * (a, b) = (1, 0)$ for all $(a, b) \in X$.

(b) Determine the following conjugates in $(X, *)$

(i) $(3, 2) * (1, 7) * (3, 2)^{-1}$ (ii) $(-1, 3) * (1, -2) * (-1, 3)^{-1}$

(c) In the same worked exercise, Worked Exercise B18, you also saw that the set

$$A = \{(1, b) : b \in \mathbb{R}\}$$

is a subgroup of the group $(X, *)$.

Use Theorem E28 to prove that this subgroup A is normal in $(X, *)$.

Hint: Remember that a general element of X is of the form (c, d), say, where $c, d \in \mathbb{R}$ and $c \neq 0$, and a general element of A is of the form $(1, b)$, say, where $b \in \mathbb{R}$.

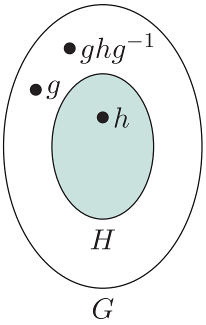


Figure 23 A subgroup H that is not normal in a group G: there is an element h of H and an element g of G such that conjugating h by g does not give an element of H

The characterisation of normal subgroups in Theorem E28 also provides a useful means of showing that a subgroup H of a group G is *not* normal in G. To do this, we have to show that H and G do not satisfy the condition in the theorem, by giving a counterexample. That is, we have to find *one* element h in H and *one* element g in G such that the conjugate ghg^{-1} does not belong to H, as illustrated in Figure 23.

Worked Exercise E29

Use Theorem E28 to show that the subgroup

$$H = \langle r \rangle = \{e, r\}$$

of $S(\square)$ is not a normal subgroup of $S(\square)$.

(The group table of $S(\square)$ is given as Table 9.)

Table 9 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

Solution

By experimentation, we find an element $g \in S(\square)$ and an element $h \in H$ such that the conjugate $g \circ h \circ g^{-1}$ does not belong to H. We can ignore e as a possibility for the element of H, since $g \circ e \circ g^{-1} = e$ for all $g \in S(\square)$, so the only possibility for the element of H is r.

We have $r \in H$ and $a \in S(\square)$, but

$$a \circ r \circ a^{-1} = t \notin H.$$

Therefore by Theorem E28 the subgroup H is not normal in G.

Exercise E83

Use Theorem E28 to prove that the following subgroups of S_4 are not normal subgroups of S_4.

(a) $H = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$, the symmetry group of the rectangle when its edges are labelled as shown in Figure 24.

(b) $H = \{g \in S_4 : g(2) = 2\}$, the subgroup of all permutations in S_4 that fix the symbol 2.

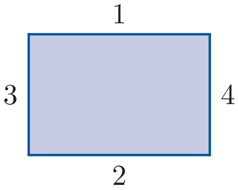


Figure 24 A rectangle with labelled edges

Exercise E84

Let $(X, *)$ be the group defined in Exercise E82.

Show that the subset

$$K = \{(1, n) : n \in \mathbb{Z}\}$$

of X is a subgroup of X, and determine whether it is a normal subgroup of X.

3.2 Conjugate subgroups

In this subsection you will see that the idea of *conjugate subgroups*, which you met in the context of symmetric groups in Unit B3, can be extended to other groups. This leads to another characterisation of normal subgroups.

In Subsection 4.2 of Unit B3 you met the idea of conjugating a whole subgroup H of a symmetric group S_n by a permutation g in S_n, as follows.

Notation

Let H be a subgroup of S_n, and let g be any permutation in S_n. Then

$g \circ H \circ g^{-1}$ denotes the set $\{g \circ h \circ g^{-1} : h \in H\}$.

That is, $g \circ H \circ g^{-1}$ is the set obtained by conjugating every element of H by the permutation g.

You saw that if H is a subgroup of S_n, then for every permutation g in S_n the set $g \circ H \circ g^{-1}$ is also a subgroup of S_n: this is Theorem B65 in Unit B3. We say that the subgroup $g \circ H \circ g^{-1}$ is a **conjugate subgroup** of H in S_n.

We can extend these ideas to groups in general. We use the following notation.

Notation

Let H be a subgroup of a group G, and let g be any element of G. Then

gHg^{-1} denotes the set $\{ghg^{-1} : h \in H\}$.

That is, gHg^{-1} is the set obtained by conjugating every element of H by the element g.

The theorem below generalises Theorem B65 from symmetric groups to all groups.

Theorem E29

Let H be a subgroup of a group G and let g be any element of G. Then the subset gHg^{-1} is a subgroup of G.

Proof We check the three subgroup properties.

SG1 Closure Consider any two elements of gHg^{-1}; we can write them as ghg^{-1} and gkg^{-1} where $h, k \in H$. We have

$$\begin{aligned}(ghg^{-1})(gkg^{-1}) &= gh(g^{-1}g)kg^{-1}\\ &= ghekg^{-1}\\ &= ghkg^{-1}.\end{aligned}$$

This is an element of gHg^{-1} because hk is an element of H (since H is a subgroup of G and therefore closed under the binary operation of G). Thus gHg^{-1} is closed under the binary operation of G.

SG2 Identity The identity permutation e is in gHg^{-1} since $e = geg^{-1}$ and $e \in H$.

SG3 Inverses Consider any element of gHg^{-1}; we can write it as ghg^{-1} where $h \in H$. We have

$$\begin{aligned}(ghg^{-1})^{-1} &= (g^{-1})^{-1}h^{-1}g^{-1}\\ &\qquad \text{(by Proposition B14 in Unit B1, applied twice)}\\ &= gh^{-1}g^{-1}.\end{aligned}$$

This is an element of gHg^{-1} because h^{-1} is an element of H (since H is a subgroup of G and therefore contains the inverse of each of its elements). Thus gHg^{-1} contains the inverse of each of its elements.

Since gHg^{-1} satisfies the three subgroup properties, it is a subgroup of G. ■

We can now make the following definitions.

Definitions

Let H be a subgroup of a group G and let g be an element of G. We call the subgroup gHg^{-1} the **conjugate subgroup** of H by g. We also say that

- gHg^{-1} is a **conjugate subgroup** of H in G
- g **conjugates** H to gHg^{-1}.

Although we used notation of the form $g \circ H \circ g^{-1}$ for conjugate subgroups (in symmetric groups) in Unit B3, in Book E we will use notation of the form gHg^{-1}, for brevity, even if we are using the symbol $\circ$ to denote the binary operation.

Worked Exercise E30

Let H be the subgroup $\langle t \rangle = \{e, t\}$ of $S(\triangle)$. Determine the conjugate subgroup aHa^{-1}.

(The non-identity elements of $S(\triangle)$ are shown in Figure 25, and the group table of $S(\triangle)$ is given as Table 10.)

Solution

We have

$$aHa^{-1} = \{a \circ e \circ a^{-1}, a \circ t \circ a^{-1}\}.$$

Now

$$\begin{aligned} a \circ e \circ a^{-1} &= a \circ a^{-1} = e, \\ a \circ t \circ a^{-1} &= (a \circ t) \circ b = s \circ b = r. \end{aligned}$$

So

$$aHa^{-1} = \{e, r\}.$$

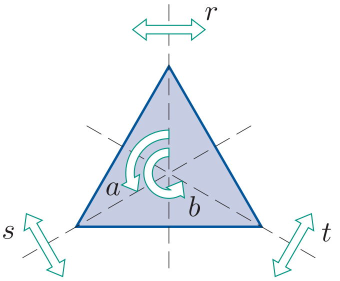


Figure 25 The symmetries of the equilateral triangle

Table 10 $S(\triangle)$

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

Exercise E85

Determine the conjugate subgroup gHg^{-1} in the group $S(\square)$ in each of the following cases.

(a) $H = \langle s \rangle = \{e, s\}$ and $g = a$ (b) $H = \{e, b, s, u\}$ and $g = r$

(The group table of $S(\square)$ is given as Table 11. You saw that the set H in part (b) is a subgroup of $S(\square)$ in Exercise E15 in Subsection 1.4 of Unit E1.)

Table 11 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

In Subsection 2.2 you saw that if x and y are elements of a group G and the element g of G conjugates x to y, then g^{-1} conjugates y to x. It follows that if H and K are subgroups of a group G, and the element g of G conjugates H to K, then g^{-1} conjugates K to H. Because of this, instead of saying that K is a conjugate subgroup of H in G, we can simply say that H and K are **conjugate subgroups** in G.

Conjugate subgroups have the following property.

Proposition E30

Let H and K be conjugate subgroups in a group G. Then either H and K have the same finite order, or they both have infinite order.

Proof Since H and K are conjugate subgroups in G, there is an element g of G such that $K = gHg^{-1}$. Consider the following mapping:

$$\begin{aligned} \phi : H &\longrightarrow K \\ x &\longmapsto gxg^{-1}. \end{aligned}$$

This mapping ϕ is onto, since every element of K is of the form gxg^{-1} where $x \in H$. Also, it is one-to-one, since if $x, y \in H$ and $gxg^{-1} = gyg^{-1}$ then $x = y$, by the Cancellation Laws.

Thus ϕ is a one-to-one correspondence, which proves the required result. ■

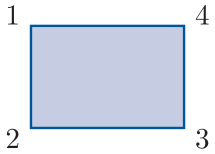


Figure 26 A labelled rectangle

Exercise E86

Consider the following subgroup K of A_4:

$$K = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

(It is the symmetry group of the rectangle when its vertices are labelled in the usual way, as shown in Figure 26.)

(a) By conjugating each element of K individually, determine the following conjugate subgroups of K in A_4.

(i) $(1\ 2\ 4)K(1\ 2\ 4)^{-1}$ (ii) $(2\ 4\ 3)K(2\ 4\ 3)^{-1}$

(b) Without calculating any further conjugates, determine how many different conjugate subgroups K has in A_4.

Hint: Remember that conjugating a permutation does not change its cycle structure.

You saw in Exercise E86(b) that the subgroup

$$K = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

of the group A_4 has the property that

$$gKg^{-1} = K \quad \text{for each element } g \in A_4.$$

In other words, conjugating K by any element of A_4 just gives K again. You also saw in Exercise E47 in Section 5 of Unit E1 that this same subgroup K is a normal subgroup of A_4.

These two properties of this subgroup K are linked: it turns out that if a subgroup H of a group G has the property that conjugating H by any element of G always gives H again, then H is normal in G, and that the converse of this result also holds. That is, we have the theorem below. This theorem provides our second alternative characterisation of normality. It is proved in Subsection 3.4.

Theorem E31

Let G be a group and let H be a subgroup of G. Then H is a normal subgroup of G if and only if

$$gHg^{-1} = H \quad \text{for each } g \in G.$$

You may be wondering whether Theorem E31 is really just another way of expressing Theorem E28, our previous characterisation of normality. However, Theorem E28 can be expressed as follows, which shows that Theorem E31 is not quite the same.

Theorem E28 (expressed differently)

Let G be a group and let H be a subgroup of G. Then H is a normal subgroup of G if and only if

$$gHg^{-1} \subseteq H \quad \text{for each } g \in G.$$

The characterisation of normality in Theorem E31 is interesting, but it turns out to be less useful in practice than the other two new characterisations given in this section.

3.3 Normal subgroups and conjugacy classes

This subsection gives the third of our three alternative characterisations of normality. It is closely related to the characterisation given in the previous subsection, but more useful in practice.

Recall that the *conjugacy class* of an element x in a group G is the subset of G consisting of all the elements of G that are conjugate to x:

$$\{gxg^{-1} : g \in G\}.$$

It can contain just the element x itself, or it can contain x together with further elements. The distinct conjugacy classes of the elements of a group G partition G, and we refer to them as the conjugacy classes of G.

Now suppose that H is a normal subgroup of a group G. We know from Theorem E28 (our first alternative characterisation of normality) that if $h \in H$ then every conjugate of h in G belongs to H. In other words, if $h \in H$ then the entire conjugacy class of h in G is a subset of H.

So each conjugacy class of G is either wholly inside H or wholly outside H: it cannot lie partly inside and partly outside.

So the following statement holds:

> A normal subgroup is a union of conjugacy classes.

(Here a 'union of conjugacy classes' includes the possibility of a trivial union of just one class.)

It turns out that the following statement is also true:

> Any subgroup of G that is a union of conjugacy classes of G is a normal subgroup of G.

Together these two facts give the following third alternative characterisation of normal subgroups. It is illustrated in Figures 27 and 28. As with the earlier characterisations, it is proved in Subsection 3.4.

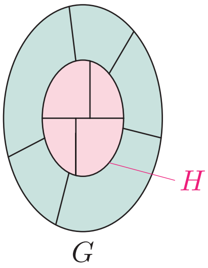


Figure 27 A normal subgroup H of a group G: each conjugacy class of G lies either entirely inside or entirely outside H

Theorem E32

Let G be a group and let H be a subgroup of G. Then H is a normal subgroup of G if and only if

H is a union of conjugacy classes of G.

By Theorem E32, if we know the conjugacy classes of a group G, then we can use them to determine whether any subgroup of G is normal in G. In the remainder of this subsection we will look at several examples that illustrate this use of Theorem E32.

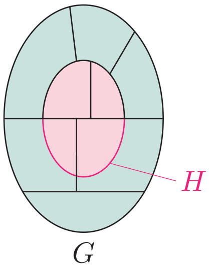


Figure 28 A subgroup H of a group G that is not normal: some conjugacy classes of G lie partly inside and partly outside H

Worked Exercise E31

Given that the subgroups of $S(\square)$ are as follows, find all the normal subgroups of $S(\square)$.

Order	Subgroup
1	$\{e\}$
2	$\{e,b\}$, $\{e,r\}$, $\{e,s\}$, $\{e,t\}$, $\{e,u\}$
4	$\{e,a,b,c\}$, $\{e,b,r,t\}$, $\{e,b,s,u\}$
8	$S(\square)$

Solution

In Worked Exercise E28 in Subsection 2.3 we found that the conjugacy classes of $S(\square)$ are

$$\{e\}, \quad \{a,c\}, \quad \{b\}, \quad \{r,t\}, \quad \{s,u\}.$$

Six of the ten subgroups of $S(\square)$ are unions of conjugacy classes, as follows.

$$
\begin{aligned}
&\{e\} = \{e\}\\
&\{e,b\} = \{e\} \cup \{b\}\\
&\{e,a,b,c\} = \{e\} \cup \{a,c\} \cup \{b\}\\
&\{e,b,r,t\} = \{e\} \cup \{b\} \cup \{r,t\}\\
&\{e,b,s,u\} = \{e\} \cup \{b\} \cup \{s,u\}\\
&S(\square) = \{e\} \cup \{a,c\} \cup \{b\} \cup \{r,t\} \cup \{s,u\}
\end{aligned}
$$

Hence by Theorem E32 these six subgroups are normal subgroups of $S(\square)$.

The remaining four subgroups $\{e,r\}$, $\{e,s\}$, $\{e,t\}$ and $\{e,u\}$ of $S(\square)$ are not normal, since none of them can be expressed as a union of conjugacy classes.

Exercise E87

Given that the subgroups of the group $S(\triangle)$ are as follows, find all the normal subgroups of $S(\triangle)$.

Order	Subgroup
1	$\{e\}$
2	$\{e,a,b\}$
3	$\{e,r\}$, $\{e,s\}$, $\{e,t\}$
6	$S(\triangle)$

(The conjugacy classes of $S(\triangle)$ are

$$\{e\}, \quad \{a,b\}, \quad \{r,s,t\}.$$

You were asked to find them in Exercise E77 in Subsection 2.3.)

In each of Worked Exercise E31 and Exercise E87 we found all the normal subgroups of a finite group by starting with all the subgroups and working out which of them are unions of conjugacy classes. However, often we do not know all the subgroups of a group or there may be a large number of them, so it can be better to instead start with the conjugacy classes and work out which unions of conjugacy classes are subgroups. We can immediately dismiss as possibilities any unions of conjugacy classes that do not contain the identity element. We can also immediately dismiss any unions of conjugacy classes whose total number of elements is not a divisor of the order of G, in view of Lagrange's Theorem. We then need to determine which of the remaining possibilities are subgroups.

This approach is illustrated in the next worked exercise, in which we find all the normal subgroups of the symmetric group S_4. Remember that for a symmetric group the partition into conjugacy classes is the same as the partition by cycle structure (by Theorem B64, repeated in Subsection 2.1).

Worked Exercise E32

Given that the numbers of elements in the conjugacy classes of the symmetric group S_4 are as follows, determine all the normal subgroups of S_4.

Conjugacy class	Cycle structure	Number of elements
A	e	1
B	$(-\ -)$	6
C	$(-\ -\ -)$	8
D	$(-\ -\ -\ -)$	6
E	$(-\ -)(-\ -)$	3

(The numbers of elements of S_4 with cycle structures e, $(-\ -\ -)$ and $(-\ -)(-\ -)$ were worked out in Subsection 3.3 of Unit B3. The numbers of elements with cycle structures $(-\ -)$ and $(-\ -\ -\ -)$ can be worked out in similar ways.)

Solution

We have to work out which unions of conjugacy classes are subgroups. We can start by narrowing down the possibilities to unions that include the class $A = \{e\}$ and that contain a total of 1, 2, 3, 4, 6, 8, 12 or 24 elements (since the order of S_4 is $4! = 24$). So, for example, we can dismiss $B \cup D$, as it does not include the identity element e, and we can dismiss $A \cup B$, as it contains $1 + 6 = 7$ elements.

To draw up a list of unions of conjugacy classes that might possibly be subgroups, we need to find all the ways of adding up some of the numbers

1, 3, 6, 6, 8

(the sizes of the conjugacy classes), always including 1, to give a total of 1, 2, 3, 4, 6, 8, 12 or 24.

There is one way to obtain the total 1, namely 1 itself.

The smallest possible total greater than 1 that can be achieved with the given numbers including 1 is 4, so neither of the totals 2 or 3 is possible.

There is one way to obtain the total 4, namely $1 + 3 = 4$.

Since only one of the given numbers other than 1 is odd, namely 3, any even total must include both the numbers 1 and 3. The smallest such total that can be achieved is $1 + 3 = 4$, and adding the next smallest number, 6, gives $1 + 3 + 6 = 10$, so neither of the totals 6 and 8 is possible.

There is one way to obtain the total 12, namely $1 + 3 + 8 = 12$.

There is one way to obtain the total 24, namely $1 + 3 + 6 + 6 + 8 = 24$.

Thus there are four suitable sums of numbers:

$$1, \quad 1 + 3 = 4, \quad 1 + 3 + 8 = 12, \quad 1 + 3 + 6 + 6 + 8 = 24.$$

So the only unions of conjugacy classes that include $A = \{e\}$ and have a permissible number of elements are as follows:

A	(1 element),
$A \cup E$	(4 elements),
$A \cup C \cup E$	(12 elements),
$A \cup B \cup C \cup D \cup E$	(24 elements).

If any of these sets is a subgroup, then it is a normal subgroup, by Theorem E32.

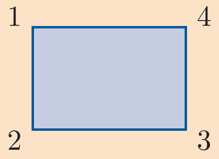
We can use any means to determine which of these sets are subgroups.

The first and fourth of these sets are the set $\{e\}$ and the whole set S_4 respectively, so both of these are subgroups.

The second set contains e and all the permutations in S_4 with cycle structure $(-\ -)(-\ -)$, so it is

$$\{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

This set is the symmetry group of a rectangle with vertex locations labelled in the usual way, as shown below, so it is a subgroup.



The third set contains all the permutations in S_4 with cycle structure e, $(-\ -\ -)$ or $(-\ -)(-\ -)$, that is, all the even permutations in S_4. Thus it is the alternating group A_4, so it is a subgroup.

Thus the normal subgroups of S_4 are

$$\{e\}, \quad \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}, \quad A_4, \quad S_4.$$

The method used in Worked Exercise E32 is summarised below. Remember that the notation $|G|$, where G is a group, denotes the order of G.

Strategy E5

To find all the normal subgroups of a finite group G, do the following.

1. Partition G into conjugacy classes.
2. Find all the unions of conjugacy classes that include the class $\{e\}$ and whose total number of elements is a divisor of $|G|$.
3. Determine whether each such union of conjugacy classes is a subgroup of G: any union that is a subgroup is a normal subgroup of G.

In the next exercise you are asked to find all the normal subgroups of the alternating group A_5. Before you can do this, you need to know the conjugacy classes of A_5. Since A_5 is a subgroup of S_5, any two elements of A_5 that are conjugate in A_5 are also conjugate in S_5 and hence have the same cycle structure. Therefore we can find the conjugacy classes of A_5 by first partitioning A_5 by cycle structure and then determining whether each cycle structure class is a conjugacy class of A_5 or whether it splits into two or more conjugacy classes. If we do this (the details are not included here), then we find that A_5 has four cycle structure classes, and only one of these splits further, into two conjugacy classes, so A_5 has five conjugacy classes. These are described in the exercise below.

Exercise E88

Given that the conjugacy classes of the alternating group A_5 are as follows, determine all the normal subgroups of A_5.

Conjugacy class	Description	Number of elements
A	e	1
B	3-cycles	20
C	products of two transpositions	15
D	5-cycles conjugate to $(1\ 2\ 3\ 4\ 5)$	12
E	5-cycles conjugate to $(1\ 2\ 3\ 5\ 4)$	12

3.4 Proofs of the theorems characterising normality

Each of Theorems E28, E31 and E32, in Subsections 3.1, 3.2 and 3.3, respectively, gives a property that characterises normal subgroups. The three theorems are all summarised in the following theorem, which includes the three properties labelled as Properties B, C and D, and the property from the original definition of a normal subgroup expressed algebraically and labelled as Property A. The algebraic version of the property from the original definition was given in Proposition E13.

Theorem E33

A subgroup H of a group G is normal in G if and only if it has any one of the following equivalent properties.

Property A $gH = Hg$ for each $g \in G$.

Property B $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$.

Property C $gHg^{-1} = H$ for each $g \in G$.

Property D H is a union of conjugacy classes of G.

Although Property A was used in the original definition of a normal subgroup, any of the other three conditions could have been used in its place. We can use any of the four conditions when we wish to prove that a subgroup is normal, or show that it is not normal.

- Property A is useful when we know the partitions into left cosets and into right cosets.
- Property B is useful in many general situations.
- Property C may be helpful when we have knowledge about conjugate subgroups.
- Property D is particularly useful when we know the conjugacy classes.

As yet, you have not seen proofs of Theorems E28, E31 and E32; that is, you have not seen a proof that the four conditions are equivalent. The remainder of this subsection provides the missing proofs.

Outline of the proof

Rather than prove the three theorems individually, we will prove that if H is a subgroup of a group G, then the following five implications hold:

$$\text{A} \implies \text{C}, \quad \text{C} \implies \text{A}, \quad \text{B} \implies \text{C}, \quad \text{C} \implies \text{D}, \quad \text{D} \implies \text{B}.$$

Here A, B, C and D stand for Properties A, B, C and D, respectively.

The five implications are illustrated in Figure 29. It follows from these five implications that any one of the four conditions is equivalent to any other. For example, the equivalence of conditions A and B, which we can write as A $\iff$ B, follows from

$$\text{A} \implies \text{C}, \quad \text{C} \implies \text{D}, \quad \text{D} \implies \text{B}, \quad \text{which together give A} \implies \text{B},$$

and

$$\text{B} \implies \text{C}, \quad \text{C} \implies \text{A}, \quad \text{which together give B} \implies \text{A}.$$

$$\begin{tikzcd}
 & & \text{B} \arrow[dl, Rightarrow] \\
\text{A} \arrow[r, Leftrightarrow] & \text{C} \arrow[dr, Rightarrow] & \\
 & & \text{D} \arrow[uu, Rightarrow]
\end{tikzcd}$$

Figure 29 The five implications proved in the proof of Theorem E33

You may be wondering why we prove the five implications above, when we could prove Theorem E33 by proving just four implications, such as

$$\text{A} \implies \text{B}, \quad \text{B} \implies \text{C}, \quad \text{C} \implies \text{D}, \quad \text{D} \implies \text{A}.$$

The reason is that the five chosen implications are more straightforward to prove.

Proof of Theorem E33 Let H be a subgroup of a group G. We prove the five implications

$$\text{A} \implies \text{C}, \quad \text{C} \implies \text{A}, \quad \text{B} \implies \text{C}, \quad \text{C} \implies \text{D}, \quad \text{D} \implies \text{B},$$

where A, B, C and D stand for Properties A, B, C and D, respectively.

A $\implies$ C

Suppose that $gH = Hg$ for each $g \in G$. We have to prove that $gHg^{-1} = H$ for each $g \in G$. Let $g \in G$. Then

$$\begin{aligned}
&x \in gHg^{-1}\\
&\iff x = ghg^{-1} \text{ for some } h \in H\\
&\iff x = h_1gg^{-1} \text{ for some } h_1 \in H \quad (\text{since } gH = Hg)\\
&\iff x = h_1 \text{ for some } h_1 \in H\\
&\iff x \in H,
\end{aligned}$$

so $gHg^{-1} = H$, as required.

(You can check the sequence of equivalences ($\iff$) here by first checking all the forward implications ($\implies$) and then checking all the backward implications ($\impliedby$). The forward implications prove that $gHg^{-1} \subseteq H$, and the backward implications prove that $gHg^{-1} \supseteq H$.)

C $\implies$ A

Suppose that $gHg^{-1} = H$ for each $g \in G$. We have to prove that $gH = Hg$ for each $g \in G$. Let $g \in G$. Then

$$\begin{aligned}
&x \in gH\\
&\iff x = gh \text{ for some } h \in H\\
&\iff x = ghg^{-1}g \text{ for some } h \in H\\
&\iff x = h_1g \text{ for some } h_1 \in H \quad (\text{since } gHg^{-1} = H)\\
&\iff x \in Hg,
\end{aligned}$$

so $gH = Hg$, as required.

(You can check the sequence of equivalences here in the same way as described above. The forward implications prove that $gH \subseteq Hg$, and the backward implications prove that $gH \supseteq Hg$.)

B $\implies$ C

Suppose that $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$ (Property B). We have to prove that $gHg^{-1} = H$ for each $g \in G$. Let $g \in G$.

First we prove that $H \subseteq gHg^{-1}$. Let $h \in H$. We can write h as

$$\begin{aligned} h &= gg^{-1}hgg^{-1} \\ &= gg^{-1}h(g^{-1})^{-1}g^{-1} \quad (\text{since } g = (g^{-1})^{-1}). \end{aligned}$$

Now

$$g^{-1}h(g^{-1})^{-1} \in H,$$

by Property B, since g^{-1} is an element of G. Hence the expression for h above shows that

$$h \in gHg^{-1}.$$

Thus $H \subseteq gHg^{-1}$, as required.

It follows immediately from Property B that $gHg^{-1} \subseteq H$, so $gHg^{-1} = H$, as required.

C $\implies$ D

Suppose that $gHg^{-1} = H$ for each $g \in G$. We have to prove that H is a union of conjugacy classes of G.

Let h be any element of H. For any element $g \in G$, we have $ghg^{-1} \in gHg^{-1}$, and hence, since $gHg^{-1} = H$, we have $ghg^{-1} \in H$. Thus H contains every conjugate in G of each of its elements; that is, H is a union of conjugacy classes of G.

D $\implies$ B

Suppose that H is a union of conjugacy classes of G. We have to prove that $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$. For each $h \in H$ and each $g \in G$, the element ghg^{-1} lies in the conjugacy class of h and hence, since H is a union of conjugacy classes of G, it lies in H, as required.

It follows from the five implications proved above that Properties A, B, C and D are all equivalent to each other. Since by definition a subgroup H of a group G is normal in G if and only if it has Property A, this proves the theorem. ■

4 Conjugacy in symmetry groups

For some groups it is possible to say what conjugacy 'means' in the particular context of that group. For example, you have seen that in a symmetric group two elements are conjugate if and only if they have the same cycle structure. In this section you will see how we can interpret conjugacy in symmetry groups.

4.1 Conjugacy and geometric type

In Subsection 2.3 we found that the conjugacy classes of the symmetry group $S(\square)$ (see Figure 30) are as listed on the left below. Notice that these classes bring together symmetries of similar geometric type, as described on the right:

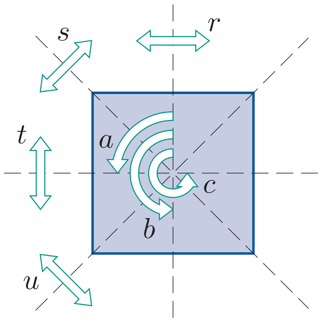


Figure 30 $S(\square)$

$\{e\}$	identity
$\{b\}$	rotation through π
$\{a, c\}$	anticlockwise and clockwise rotations through $\pi/2$
$\{s, u\}$	reflections in diagonal axes
$\{r, t\}$	reflections in axes parallel to edges.

(The rotation c is described here as a clockwise rotation through $\pi/2$ rather than as an anticlockwise rotation through $3\pi/2$ to highlight its geometric similarity to the rotation a.)

We also found in Subsection 2.3 that the conjugacy classes of the symmetry group $S(\triangle)$ (see Figure 31) are as listed on the left below. Again these classes bring together symmetries of similar geometric type, as described on the right:

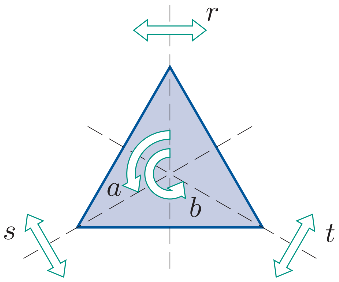


Figure 31 $S(\triangle)$

$\{e\}$	identity
$\{a, b\}$	anticlockwise and clockwise rotations through $2\pi/3$
$\{r, s, t\}$	reflections in axes through vertices and midpoints of edges.

As suggested by these examples, there is a link between conjugacy and geometric type in symmetry groups. To see why this is so, you need to understand what happens when you conjugate one element of a symmetry group by another. It can be quite difficult to picture this, but to try to give you some insight into it we will now look at two examples in $S(\square)$. As in Unit B1, we will track the position of the square by picturing it as a paper model coloured light blue on one side and darker blue on the other, with a dot in the same corner on both sides (as if it goes through the paper).

You will need to think about these examples quite carefully. If you find them hard to understand, then skip them for the moment and go on to the box headed 'Conjugation in a symmetry group': you should be able to apply the statement there even if you do not fully understand why it holds. Try returning to the two examples once you have completed Exercises E89 and E90.

As a first example, consider Figure 32, which shows the effect of the conjugate symmetry $r \circ a \circ r^{-1}$. To apply this conjugate symmetry, we first apply r^{-1}, which reflects the square in the vertical axis, then a, which rotates the square anticlockwise through $\pi/2$, then finally r, which 'reflects the square back again'. Since the rotation through $\pi/2$ anticlockwise was done *when the square was in a reflected position*, the overall effect is to rotate through $\pi/2$ *clockwise*, that is to apply the symmetry c.

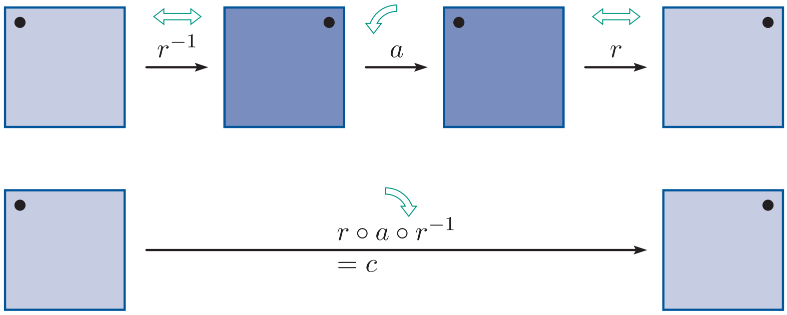


Figure 32 The effect of the conjugate symmetry $r \circ a \circ r^{-1}$ on the square

Thus the conjugate symmetry $r \circ a \circ r^{-1}$ is the symmetry obtained by 'applying r to the *action* of a', as illustrated in Figure 33.

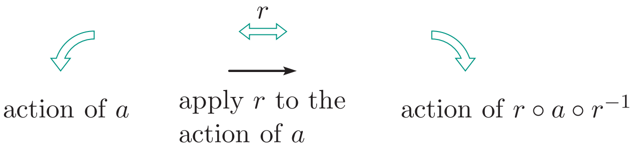

action of a
r
apply r to the action of a
action of $r \circ a \circ r^{-1}$

Figure 33 Conjugating a by r

(Note that here the word 'action' is used in its everyday sense, not in the sense of a 'group action', a concept that you will meet in Unit E4.)

As another example, consider Figure 34, which shows the effect of the conjugate symmetry $a \circ s \circ a^{-1}$. To apply this conjugate symmetry, we first apply a^{-1}, which rotates the square clockwise through $\pi/2$, then s, which reflects the square in the top left to bottom right diagonal axis, then finally a, which 'rotates the square back again'. Since the reflection in the top left to bottom right axis was done *when the square was rotated clockwise by* $\pi/2$, the overall effect is to reflect in the line obtained by rotating this axis anticlockwise by $\pi/2$, which is the top right to bottom left axis – that is, the overall effect is to apply the symmetry u.

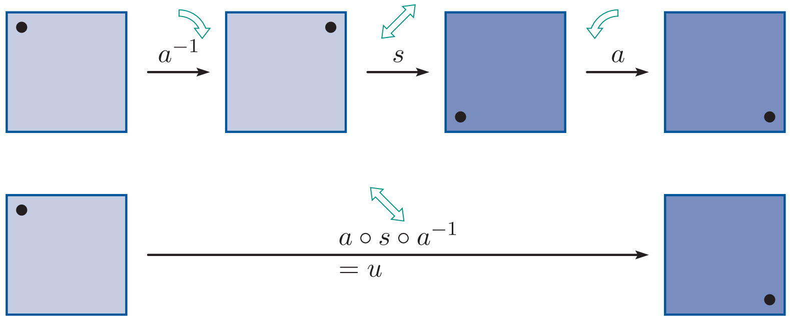


Figure 34 The effect of the conjugate symmetry $a \circ s \circ a^{-1}$ on the square

Thus the conjugate symmetry $a \circ s \circ a^{-1}$ is the symmetry obtained by 'applying a to the *action* of s', as illustrated in Figure 35.

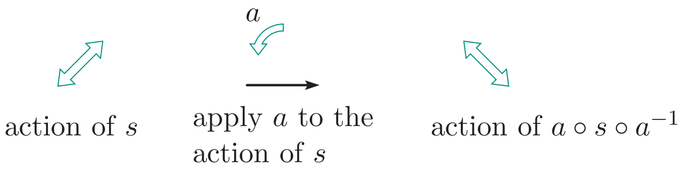

a
action of s
apply a to the action of s
action of $a \circ s \circ a^{-1}$

Figure 35 Conjugating s by a

In general, for any symmetries x and g of a figure F, the conjugate symmetry $g \circ x \circ g^{-1}$ is the symmetry obtained by 'applying g to the *action* of x'. This leads to the following helpful informal way to think about conjugacy in symmetry groups.

Conjugation in a symmetry group

Let x and g be symmetries of a figure F. Then $g \circ x \circ g^{-1}$ is the symmetry that is illustrated by the diagram obtained when g is applied to a diagram illustrating x (if we ignore any labels).

For example, in Figure 37 the symmetry r of the square (reflection in the vertical axis) is applied to a diagram for the symmetry a. By the statement in the box above, the resulting diagram illustrates the symmetry $r \circ a \circ r^{-1}$. We can see that the resulting diagram illustrates the symmetry c (see Figure 36), so $r \circ a \circ r^{-1} = c$.

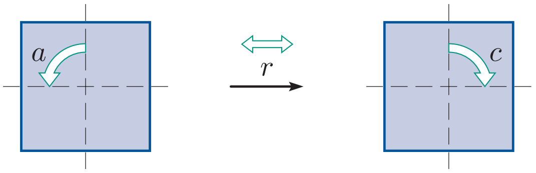


Figure 37 The conjugate symmetry $r \circ a \circ r^{-1}$ is equal to c

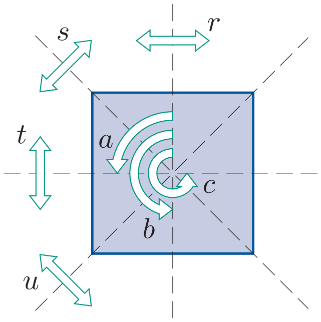


Figure 36 $S(\square)$

Similarly, in Figure 38 the symmetry a of the square (anticlockwise rotation through $\pi/2$) is applied to a diagram for the symmetry s. By the statement in the box above, the resulting diagram illustrates the symmetry $a \circ s \circ a^{-1}$. We can see that the resulting diagram illustrates the symmetry u, so $a \circ s \circ a^{-1} = u$.

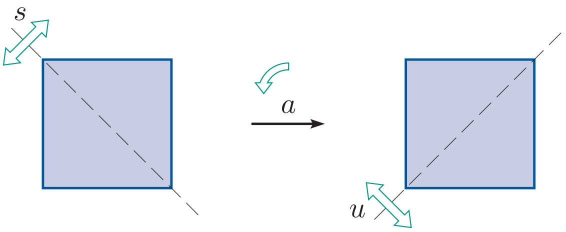


Figure 38 The conjugate symmetry $a \circ s \circ a^{-1}$ is equal to u

If two symmetries x and y are conjugate in a symmetry group, then there is often more than one symmetry that conjugates x to y.

For example, Figure 38 above illustrates that a conjugates s to u in $S(\square)$, and Figure 39 below illustrates that c (anticlockwise rotation through $3\pi/2$, or, equivalently, clockwise rotation through $\pi/2$) does the same job.

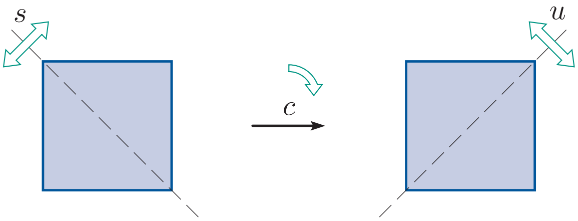


Figure 39 The conjugate symmetry $c \circ s \circ c^{-1}$ is equal to u

Figure 40 illustrates that r (reflection in the vertical axis) also does the same job.

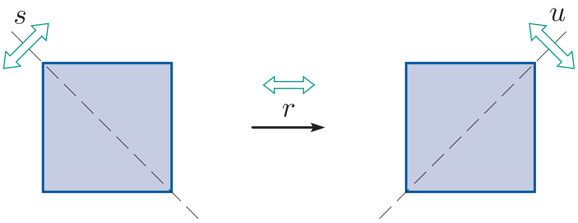


Figure 40 The conjugate symmetry $r \circ s \circ r^{-1}$ is equal to u

Make sure that you do not confuse the informal idea of a symmetry being applied to a diagram illustrating a symmetry, as in Figures 37–40, with the idea of *composing two symmetries*. For example, Figure 40 above *does not* show the symmetries s and r being composed to form the composite symmetry $r \circ s$.

The box below summarises how to use the informal ideas above to determine whether two symmetries of a figure are conjugate.

Conjugate elements in the symmetry group of a figure

- Two symmetries x and y of a figure F are conjugate in $S(F)$ if and only if there is a symmetry g of F that transforms a diagram illustrating x into a diagram illustrating y (when we ignore any labels).
- If such a symmetry g exists, then $y = g \circ x \circ g^{-1}$.

For example, Figure 37 above shows that a and c are conjugate in $S(\square)$, and Figure 38 above shows that s and u are conjugate in $S(\square)$. By way of contrast, consider the symmetries r and s in $S(\square)$ (reflection in an axis through the midpoints of opposite edges and reflection in a diagonal, respectively), as shown in Figure 41. There is no symmetry of the square that transforms a diagram illustrating r into one illustrating s, so r and s are not conjugate in $S(\square)$.

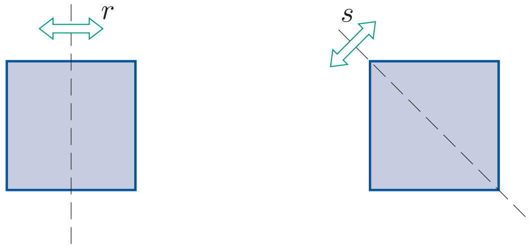


Figure 41 Diagrams illustrating the symmetries r and s of the square

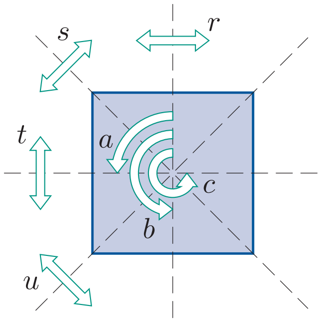


Figure 42 $S(\square)$

Exercise E89

For each of the following pairs of symmetries in $S(\square)$ (see Figure 42), use the ideas in the box above to determine whether the two symmetries are conjugate in $S(\square)$, and to write down a symmetry that conjugates the first symmetry in the pair to the second if they are conjugate.

(a) r and t (b) a and b (c) r and u

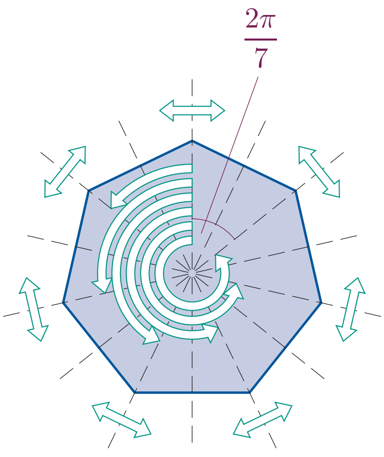
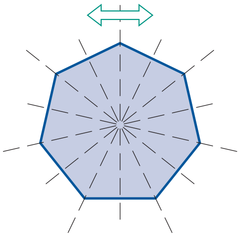
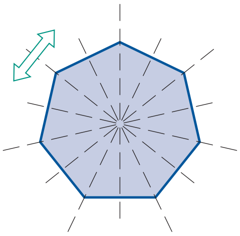


Figure 43 S(heptagon)

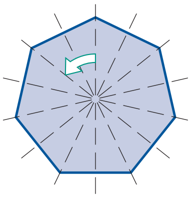
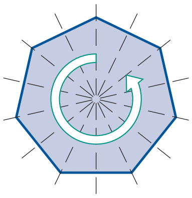
Exercise E90

For each of the following pairs of symmetries of the regular heptagon (see Figure 43), use the ideas in the box above to determine whether the two symmetries are conjugate in S(heptagon), and to describe a symmetry that conjugates the first symmetry in the pair to the second if they are conjugate.

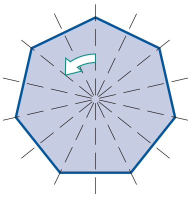
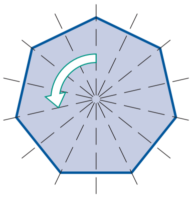
(a) Reflection in the vertical axis and reflection in the axis obtained by rotating the vertical axis by $2\pi/7$ anticlockwise.

(b) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $12\pi/7$.

(c) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $4\pi/7$.

The ideas in the box above explain the link between conjugacy and geometric type that you saw for $S(\square)$ and $S(\triangle)$.

These ideas apply to figures in $\mathbb{R}^3$ as well as to plane figures, but for such figures we have to think in terms of 'three-dimensional diagrams'.

For example, the two reflectional symmetries x and y of the tetrahedron in Figure 44 are conjugate, because there is a rotational symmetry g of the tetrahedron (about the vertical axis) which if applied to the diagram illustrating the symmetry x gives a diagram illustrating the symmetry y.

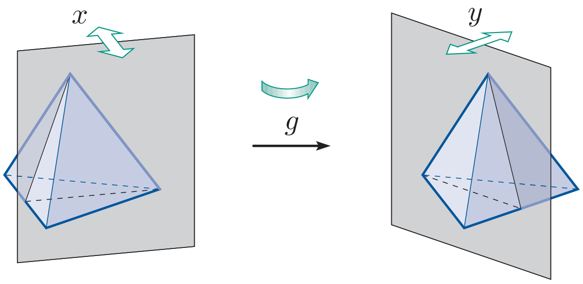


Figure 44 Two conjugate symmetries of the tetrahedron

Figure 45 may help you to understand why this is. It illustrates what happens when the symmetry x in Figure 44 is conjugated by the symmetry g mentioned above: the result is the symmetry y in Figure 44, as expected.

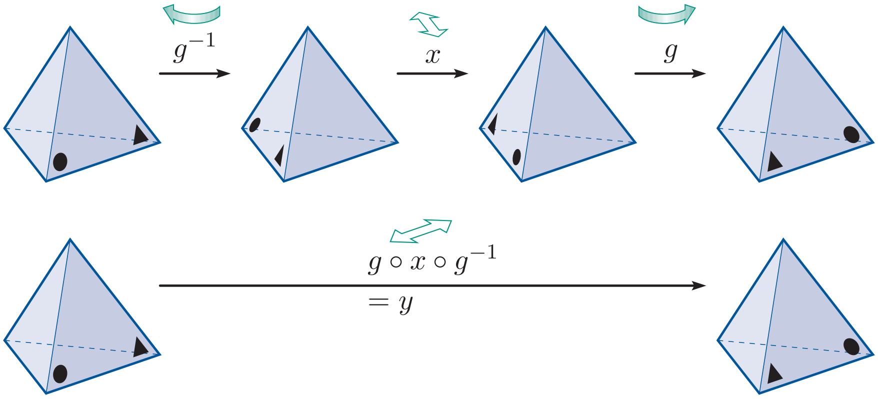


Figure 45 Two conjugate symmetries of the tetrahedron

Unfortunately it is not always practicable to determine whether symmetries of solid figures are conjugate by thinking of 'three-dimensional diagrams', because these diagrams can be difficult to picture: this applies particularly to indirect symmetries that are not reflections.

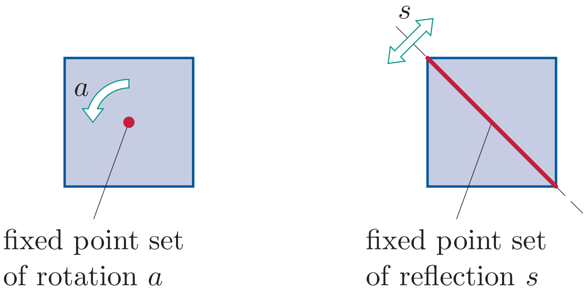
The ideas about the link between conjugacy and geometric type in symmetry groups that you have met so far in this subsection are expressed informally and were not proved rigorously, but we can formalise some of them by using the idea of the *fixed point set* of a symmetry of a figure. This is the set of points of the figure that are fixed – that is, not moved – by the symmetry.

Definition

Let f be a symmetry of a figure F. Then the **fixed point set** of f, denoted by $\operatorname{Fix} f$, is given by

$$\operatorname{Fix} f = \{P \in F : f(P) = P\}.$$

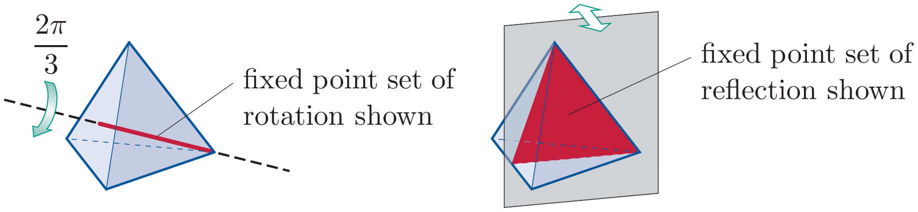
For example, the fixed point set of a non-trivial rotational symmetry of a plane figure is the centre of rotation, if this lies in the figure, and is the empty set otherwise. The fixed point set of a reflectional symmetry of a plane figure is the set of all points of the figure that lie on the axis of reflection. Figure 46 shows the fixed point sets of the rotational symmetry a and the reflectional symmetry s of the square.



a
fixed point set of rotation a
s
fixed point set of reflection s

Figure 46 The fixed point sets of two symmetries of the square

Similarly, the fixed point set of a non-trivial rotational symmetry of a solid figure is the set of all points of the figure that lie on the axis of rotation. The fixed point set of a reflectional symmetry of a solid figure is the set of all points of the figure that lie in the plane of reflection. Figure 47 shows the fixed point sets of a particular rotational symmetry and a particular reflectional symmetry of the tetrahedron.



$\frac{2\pi}{3}$
fixed point set of rotation shown
fixed point set of reflection shown

Figure 47 The fixed point sets of two symmetries of the tetrahedron

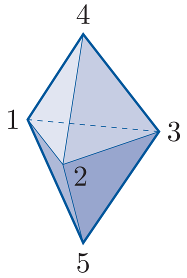
Exercise E91

Describe the fixed point set of each of the following symmetries of the double tetrahedron shown below.

(a) The reflection in the plane through vertices 3, 4 and 5.

(b) The reflection in the plane through vertices 1, 2 and 3.

(c) The rotation $(1\ 2\ 3)$.



You have seen that if x and g are symmetries of a figure F, then applying g to a diagram illustrating x gives a diagram illustrating $g \circ x \circ g^{-1}$ (when we ignore any labels). So we would expect that applying g to the fixed point set of x would give the fixed point set of $g \circ x \circ g^{-1}$. This is proved formally below.

Theorem E34

Let x and g be symmetries of a figure F, and let the fixed point set of x be L. Then the fixed point set of $g \circ x \circ g^{-1}$ is $g(L)$.

Proof Throughout this proof we use the fact that if f_1 and f_2 are symmetries of F, then

$$(f_2 \circ f_1)(P) = f_2(f_1(P)) \quad \text{for each point } P \in F.$$

This is just by the definition of $f_2 \circ f_1$.

To prove the theorem we have to show that two sets are equal: $g(L)$ and the fixed point set of $g \circ x \circ g^{-1}$.

First we show that $g(L)$ is a subset of the fixed point set of $g \circ x \circ g^{-1}$. Suppose that $P \in g(L)$. Then $g^{-1}(P) \in L$. Hence $g^{-1}(P)$ is fixed by x, so

$$x(g^{-1}(P)) = g^{-1}(P).$$

Taking the image of each side of this equation under g gives

$$g(x(g^{-1}(P))) = g(g^{-1}(P)),$$

that is,

$$(g \circ x \circ g^{-1})(P) = P.$$

Thus P is in the fixed point set of $g \circ x \circ g^{-1}$. This shows that $g(L)$ is a subset of the fixed point set of $g \circ x \circ g^{-1}$.

Now we show that the fixed point set of $g \circ x \circ g^{-1}$ is a subset of $g(L)$. Suppose that P is in the fixed point set of $g \circ x \circ g^{-1}$. Then

$$(g \circ x \circ g^{-1})(P) = P.$$

Taking the image of each side of this equation under g^{-1} gives

$$g^{-1}((g \circ x \circ g^{-1})(P)) = g^{-1}(P),$$

that is,

$$x(g^{-1}(P)) = g^{-1}(P).$$

Thus $g^{-1}(P)$ is fixed by x, so $g^{-1}(P) \in L$. Hence $P \in g(L)$. This shows that the fixed point set of $g \circ x \circ g^{-1}$ is a subset of $g(L)$.

It follows that $g(L)$ is equal to the fixed point set of $g \circ x \circ g^{-1}$, as claimed. ■

By Theorem E34, if x and y are symmetries of a figure F and we want to find a symmetry g of F that conjugates x to y, then the only symmetries worth checking to see whether they do this are the symmetries that map $\operatorname{Fix} x$ to $\operatorname{Fix} y$ (that is, the fixed point set of x to the fixed point set of y), since any other symmetry will definitely not conjugate x to y.

Note, however, that if a symmetry g maps $\operatorname{Fix} x$ to $\operatorname{Fix} y$ then there is no guarantee that it conjugates x to y: it may or may not do this.

Theorem E34 tells us in particular that if there is *no* symmetry in $S(F)$ that maps $\operatorname{Fix} x$ to $\operatorname{Fix} y$, then x and y are not conjugate.

For example, consider the two symmetries of the tetrahedron shown in Figure 48. The fixed point set of the symmetry on the left is a line segment, whereas the fixed point set of the symmetry on the right is a triangle. Hence there is no symmetry of the tetrahedron that maps the fixed point set of the symmetry on the left to the fixed point set of the symmetry on the right. It follows by Theorem E34 that the two symmetries are not conjugate.

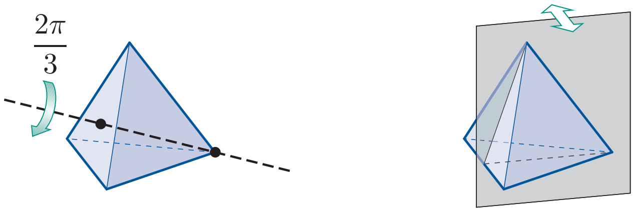


Figure 48 Two symmetries of the tetrahedron

Here is another useful result that we can sometimes apply to show that two symmetries of a figure are *not* conjugate.

Theorem E35

A direct symmetry cannot be conjugate to an indirect symmetry in a symmetry group.

Proof We use the fact that the composite of two direct symmetries or two indirect symmetries is a direct symmetry, whereas the composite of a direct symmetry and an indirect symmetry is an indirect symmetry. We also use the facts that the inverse of a direct symmetry is direct and that the inverse of an indirect symmetry is indirect.

Let x be a direct symmetry in a symmetry group and let g be any element of the group. If g is direct, then $g \circ x \circ g^{-1}$ is the composite of three direct symmetries and is therefore direct. If g is indirect, then $g \circ x \circ g^{-1}$ is the composite of a direct symmetry and two indirect symmetries and again is therefore direct. Therefore every conjugate of g is direct, which proves the theorem. ■

For example, Theorem E35 provides an even quicker method than Theorem E34 for showing that the two symmetries of the tetrahedron in Figure 48 are not conjugate. The first symmetry is a direct symmetry whereas the second symmetry is an indirect symmetry, so by Theorem E35 they are not conjugate.

4.2 Finding conjugacy classes of finite symmetry groups

In this subsection we will look at how we can find the conjugacy classes of finite symmetry groups efficiently. Remember that one reason for finding the conjugacy classes of a group is that it can help us to find its normal subgroups.

Many of the results about conjugacy that you have met can help us to work out the conjugacy classes of a symmetry group. A particularly helpful result is Proposition E26(a), from Subsection 2.3. This states that if H is a subgroup of a group G and two elements x and y of H are conjugate in H, then they must also be conjugate in G. It follows that if we represent a symmetry group $S(F)$ as a subgroup of a symmetric group S_n (by labelling the vertices of F, for example), then any symmetries that are conjugate in $S(F)$ must also be conjugate in S_n, and hence must have the same cycle structure.

So we can find the conjugacy classes of $S(F)$ by first partitioning $S(F)$ according to cycle structure, and then for each cycle structure class determining whether all the symmetries in the class are conjugate to each other or whether the class splits into two or more conjugacy classes. (Remember that the class may split because even though for any two elements x and y of $S(F)$ that have the same cycle structure there is an element g of S_n that conjugates x to y, there may not be any such element g in $S(F)$ itself.)

The strategy below sets out this approach, along with some other useful ideas.

Strategy E6

To determine the conjugacy classes of a finite symmetry group $S(F)$, do the following.

1. Represent $S(F)$ as a group of permutations.
2. Partition $S(F)$ by cycle structure.
3. For each cycle structure class, determine whether all the symmetries in the class are conjugate to each other, or whether the class splits into two or more conjugacy classes.

   The following can help you do this.

   - Two symmetries x and y are conjugate in $S(F)$ if and only if there is a symmetry g of F that transforms a diagram illustrating x into a diagram illustrating y.
   - If x and y are conjugate in a subgroup H of $S(F)$, then they are also conjugate in $S(F)$.
   - If x and y are not conjugate in a group G that has $S(F)$ as a subgroup, then they are not conjugate in $S(F)$.
   - If the fixed point set of x is L, then the fixed point set of $g \circ x \circ g^{-1}$ is $g(L)$.
   - A direct symmetry and an indirect symmetry are not conjugate.
   - Renaming method: To find the conjugate $g \circ x \circ g^{-1}$, replace each symbol in the cycle form of x by its image under g.
   - The number of elements in each conjugacy class divides $|S(F)|$.

In the next worked exercise, Strategy E6 is used to find the conjugacy classes of the symmetry group $S(\square)$ in a more efficient way than in Worked Exercise E28 in Subsection 2.3.

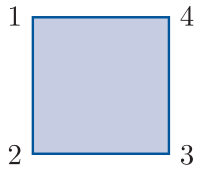


Figure 49 A labelled square

Worked Exercise E33

(a) Express the symmetries of the square as permutations in cycle form using the usual vertex labelling, as shown in Figure 49.

(b) Hence find the conjugacy classes of the symmetry group of the square.

Solution

(a) The symmetries of the square are as follows.

Rotations	Reflections
e	$(1\ 4)(2\ 3)$
$(1\ 2\ 3\ 4)$	$(2\ 4)$
$(1\ 3)(2\ 4)$	$(1\ 2)(3\ 4)$
$(1\ 4\ 3\ 2)$	$(1\ 3)$

(b) To find the conjugacy classes, first partition $S(\square)$ by cycle structure.

The partition of $S(\square)$ by cycle structure is as follows.

$$\{e\}$$

$$\{(1\ 2\ 3\ 4),\ (1\ 4\ 3\ 2)\}$$

$$\{(1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 2)(3\ 4)\}$$

$$\{(2\ 4),\ (1\ 3)\}$$

For each cycle structure class, determine whether all the symmetries in the class are conjugate to each other, or whether the class splits into two or more conjugacy classes.

One conjugacy class is $\{e\}$.

Now consider the cycle structure class

$$\{(1\ 2\ 3\ 4),\ (1\ 4\ 3\ 2)\}.$$

The symmetries $(1\ 2\ 3\ 4)$ and $(1\ 4\ 3\ 2)$ are rotations through $\pi/2$ anticlockwise and $\pi/2$ clockwise, respectively. Hence any reflection conjugates one to the other.

As a check, we can use the reflection $(1\ 4)(2\ 3)$, say, to rename one of these symmetries and check that we obtain the other:

$$(1\ 4)(2\ 3)\ \begin{array}{l}(1\ 2\ 3\ 4)\\ \ \downarrow\ \downarrow\ \downarrow\ \downarrow\\ (4\ 3\ 2\ 1) = (1\ 4\ 3\ 2),\end{array}$$

as expected.

Thus this cycle structure class is a conjugacy class.

Now consider the cycle structure class

{(1 3)(2 4), (1 4)(2 3), (1 2)(3 4)}.

The symmetry (1 3)(2 4) is not conjugate to the other two symmetries here, because it is direct whereas the other two are indirect.

The symmetries (1 4)(2 3) and (1 2)(3 4) are reflections in the vertical and horizontal axes, respectively. Hence a rotation through $\pi/2$ or $3\pi/2$ (anticlockwise) conjugates one to the other.

Check:

$$(1\ 2\ 3\ 4)\quad \begin{array}{l}(1\ 4)(2\ 3)\\ \downarrow\downarrow\ \ \ \downarrow\downarrow\\ (2\ 1)(3\ 4) = (1\ 2)(3\ 4).\end{array}$$

Thus this cycle structure class splits into two conjugacy classes:

{(1 3)(2 4)},   {(1 4)(2 3), (1 2)(3 4)}.

Finally, consider the cycle structure class

{(2 4), (1 3)}.

The symmetries (2 4) and (1 3) are reflections in diagonal axes. Hence a rotation through $\pi/2$ or $3\pi/2$ (anticlockwise) conjugates one to the other.

Check:

$$(1\ 2\ 3\ 4)\quad \begin{array}{l}(2\ 4)\\ \downarrow\downarrow\\ (3\ 1) = (1\ 3).\end{array}$$

Thus this cycle structure class is a conjugacy class.

In summary, the conjugacy classes of $S(\square)$ are as follows.

$\{e\}$

{(1 2 3 4), (1 4 3 2)}

{(1 3)(2 4)}

{(1 4)(2 3), (1 2)(3 4)}

{(2 4), (1 3)}

For some purposes we may wish to rewrite these conjugacy classes with the symmetries of the square expressed as e, a, b, c, r, s, t and u instead of in cycle form. This gives the conjugacy classes as

$$\{e\},\quad \{a,c\},\quad \{b\},\quad \{r,t\},\quad \{s,u\}.$$

In the next two exercises, you can use Strategy E6 to find the conjugacy classes of the symmetry group $S(\triangle)$ in a more efficient way than in Exercise E77 in Subsection 2.3, and to find the conjugacy classes of the symmetry group S(⬡).

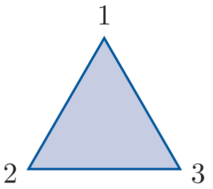


Figure 50 A labelled equilateral triangle

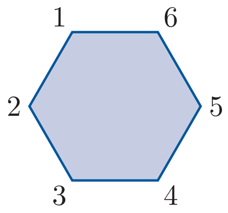
Exercise E92

(a) Express the symmetries of the equilateral triangle as permutations in cycle form using the usual vertex labelling, as shown in Figure 50.

(b) Hence find the conjugacy classes of the symmetry group of the equilateral triangle.

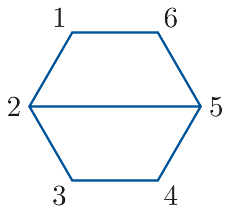
Exercise E93

(a) Express the symmetries of the regular hexagon below as permutations of the vertex labels in cycle form.



(b) Hence find the conjugacy classes of S(⬡), the symmetry group of the regular hexagon.

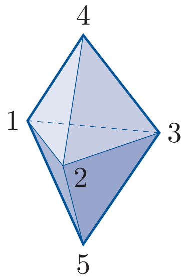
(c) Write down the subgroup of S(⬡) that is the symmetry group of the modified regular hexagon below, and use your answer to part (b) to determine whether this subgroup is normal in S(⬡).



In the next exercise you are challenged to find the conjugacy classes of the symmetry group of the double tetrahedron. This is a little trickier than the exercises so far in this subsection, as you will probably not be able to picture three-dimensional diagrams for some of the symmetries, since some of them are not simply rotations or reflections.

Exercise E94

Consider the double tetrahedron shown below.



In Worked Exercise B39 in Subsection 2.4 of Unit B3 we found that its symmetries are as follows.

e	$(4\ 5)$
$(1\ 2)$	$(1\ 2)(4\ 5)$
$(1\ 3)$	$(1\ 3)(4\ 5)$
$(2\ 3)$	$(2\ 3)(4\ 5)$
$(1\ 2\ 3)$	$(1\ 2\ 3)(4\ 5)$
$(1\ 3\ 2)$	$(1\ 3\ 2)(4\ 5)$

The symmetries in the first column are the symmetries of the double tetrahedron that arise from symmetries of the equilateral triangle with vertices labelled 1, 2 and 3 in the middle of the double tetrahedron, and the symmetries in the second column are obtained by composing the symmetries in the first column with the reflectional symmetry $(4\ 5)$ of the double tetrahedron.

Find the conjugacy classes of $S(\text{doubletet})$, the symmetry group of the double tetrahedron.

Hint: Use Strategy E6. You may wish to use the fact that the symmetry group of the double tetrahedron has $S(\triangle)$ as a subgroup.

5 Conjugacy in matrix groups

In Section 2 of Unit E1 you met the group GL(2), the **general linear group of degree** 2, whose elements are all the *invertible* 2×2 matrices with real entries, and whose binary operation is matrix multiplication.

You also met some subgroups of GL(2), including the following standard subgroups.

- The group SL(2), the **special linear group of degree** 2, whose elements are all the 2×2 matrices with determinant 1.
- The group L of all invertible 2×2 lower triangular matrices.
- The group U of all invertible 2×2 upper triangular matrices.
- The group D of all invertible 2×2 diagonal matrices.

In this section we will apply the idea of conjugacy to GL(2) and some of its subgroups.

5.1 Conjugate subgroups in matrix groups

We can use the idea of conjugacy to obtain many more subgroups of GL(2) than those you met in Unit E1. To do this, we apply the following theorem from Subsection 3.2.

Theorem E29

Let H be a subgroup of a group G and let g be any element of G. Then the subset gHg^{-1} is a subgroup of G.

We call the subgroup gHg^{-1} in Theorem E29 a **conjugate subgroup** of H in G.

A conjugate subgroup of a subgroup of GL(2) is obtained in the worked exercise below.

Worked Exercise E34

In Exercise E21(b) in Unit E1 you saw that the following set is a subgroup of GL(2):

$$P = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad = 1 \right\}.$$

(This set is specified slightly differently there.)

Find another subgroup of GL(2) by conjugating P by the matrix

$$\mathbf{B} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

Solution

Apply the definition of a conjugate subgroup,

$$gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

Conjugating P by $\mathbf{B}$ gives

$$\mathbf{B}P\mathbf{B}^{-1} = \{\mathbf{B}h\mathbf{B}^{-1} : h \in P\}$$

Replace the symbol $\mathbf{B}$ with the matrix that it denotes, and replace the symbol h with a general element of the subgroup P.

$$= \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}^{-1} : \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in P \right\}$$

The statement $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in P$ is placing a condition on what the variables a and d can be. Simplify this condition. What it says about the variables a and d is that $a, d \in \mathbb{R}$ and $ad = 1$.

$$= \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}^{-1} : a, d \in \mathbb{R},\ ad = 1 \right\}$$

Simplify the matrix product.

$$= \left\{ \begin{pmatrix} 2a & d \\ 0 & d \end{pmatrix} \times \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} : a, d \in \mathbb{R},\ ad = 1 \right\}$$

$$= \left\{ \frac{1}{2} \begin{pmatrix} 2a & -2a + 2d \\ 0 & 2d \end{pmatrix} : a, d \in \mathbb{R},\ ad = 1 \right\}$$

$$= \left\{ \begin{pmatrix} a & d - a \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad = 1 \right\}.$$

This specification of $\mathbf{B}P\mathbf{B}^{-1}$ is acceptably simple.

It is not immediately obvious that the set specified at the end of Worked Exercise E34 is a subgroup of GL(2), but by Theorem E29 we know that it is.

This subgroup is different from all the subgroups of GL(2) that you have met so far in this book. However, sometimes conjugating a subgroup of GL(2) by an element of GL(2) can give a subgroup of GL(2) that you already know about, as illustrated in the next worked exercise.

Worked Exercise E35

Consider the group U of all invertible 2×2 upper triangular matrices:

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

(a) Find the conjugate subgroup $\mathbf{C}U\mathbf{C}^{-1}$, where

$$\mathbf{C} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

(b) Show that $\mathbf{C}U\mathbf{C}^{-1}$ is equal to L, the group of all invertible 2×2 lower triangular matrices.

Solution

(a) We have

$$\begin{aligned}
\mathbf{C}U\mathbf{C}^{-1} &= \{\mathbf{C}h\mathbf{C}^{-1} : h \in U\} \\
&= \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in U \right\} \\
&= \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} 0 & -d \\ a & b \end{pmatrix} \times \frac{1}{1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} d & 0 \\ -b & a \end{pmatrix} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\}
\end{aligned}$$

We can write this specification in a slightly simpler way. As the value of the variable b varies through all the numbers in $\mathbb{R}$, so does the value of $-b$. So the specification tells us that the bottom left entry of the matrix can be any number in $\mathbb{R}$. Although we can specify this, as currently, by saying that the bottom left entry is $-b$, where $b \in \mathbb{R}$, it is simpler to say that the bottom left entry is b, where $b \in \mathbb{R}$.

$$= \left\{ \begin{pmatrix} d & 0 \\ b & a \end{pmatrix} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

(b) The group L of all invertible 2×2 lower triangular matrices is given by

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

The set specified here is the same as the set specified by the final line in the solution to part (a), because it does not matter whether we denote the bottom left entry by b or by c, and it does not matter whether we denote the top left entry by d and the bottom right entry by a or vice versa, since interchanging a and d in the conditions involving a and d leaves the conditions unchanged.

Hence, by the solution to part (a) above, $\mathbf{C}U\mathbf{C}^{-1} = L$.

Exercise E95

Recall that the group D of all invertible 2×2 diagonal matrices and the group U of all invertible 2×2 upper triangular matrices are given by

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad \neq 0 \right\},$$

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

(a) Find the conjugate subgroup

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} D \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^{-1}.$$

Is it equal to U? Justify your answer.

(b) Find the conjugate subgroup

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} U \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}.$$

Is it equal to U? Justify your answer.

Hint: Remember that to show that two sets are *not* equal you should show that there is an element of one set that is not an element of the other.

In Exercise E95(b) you should have found that conjugating the subgroup U of GL(2) by the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

gives the subgroup U again. So in this case conjugating a subgroup of GL(2) by an element of GL(2) not only gives a subgroup of GL(2) that we already knew about, but it gives the same subgroup that we conjugated. In the next exercise you are asked to show that this happens in two more cases.

Exercise E96

In Exercise E21(a) in Section 2 of Unit E1 you saw that the following set is a subgroup of GL(2):

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\}.$$

(a) Show that conjugating M by the matrix

$$\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$$

gives the subgroup M again.

(b) Show that conjugating M by the matrix

$$\begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}$$

gives the subgroup M again.

Exercise E96 might lead us to wonder whether conjugating the subgroup M in the exercise by *any* matrix in GL(2) would give the subgroup M again. If this were true, then it would mean that the subgroup M would have the property that

$$\mathbf{B}M\mathbf{B}^{-1} = M \quad \text{for each } \mathbf{B} \in \mathrm{GL}(2),$$

and hence, by Theorem E33 (Property C) in Subsection 3.4, M would be a normal subgroup of GL(2). However, in fact it is *not* true, as is shown by the first worked exercise in the next subsection, so M is *not* a normal subgroup of GL(2).

Notice, however, that both of the conjugating matrices in Exercise E96 are upper triangular matrices. It turns out that it *is* true that conjugating the subgroup M in Exercise E96 by any upper triangular matrix in GL(2), that is, by any matrix in the group U, gives the subgroup M again. In other words, the subgroup M has the property that

$$\mathbf{B}M\mathbf{B}^{-1} = M \quad \text{for each } \mathbf{B} \in U.$$

Also, M is a subgroup of U, because M is a subset of U (since every matrix in M is upper triangular) and M is a group. (The relationship between the three groups M, U and GL(2) is illustrated in Figure 51.) It follows by Theorem E33 (Property C) that M is a normal subgroup of U.

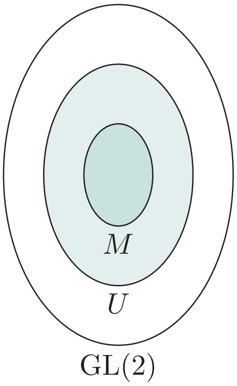


Figure 51 The relationship between the groups M, U and GL(2)

Thus M is a normal subgroup of U, but not a normal subgroup of GL(2). This is proved in the worked exercise at the start of the next subsection, where we will use Property B of Theorem E33 rather than Property C, as this makes the proof slightly easier.

5.2 Normal subgroups in matrix groups

In this subsection we will look briefly at some examples of normal subgroups in matrix groups, beginning with the example mentioned at the end of the previous subsection.

We will show that subgroups are normal (or not normal) by using Property B of Theorem E33, which is restated below for convenience.

Theorem E33 (Property B)

A subgroup H of a group G is normal in G if and only if it has the following property.

Property B: $ghg^{-1} \in H$ for each $h \in H$ and each $g \in G$.

Worked Exercise E36

Consider the following subgroup of GL(2), which appeared in Exercise E96:

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\}.$$

The relationship between M, U and GL(2) (where U is the group of all invertible 2×2 upper triangular matrices) is shown in Figure 51.

(a) Show that M is a normal subgroup of U.

(b) Show that M is not a normal subgroup of GL(2).

Solution

(a) We use Property B of Theorem E33.

We have to show that for every matrix $\mathbf{A} \in M$ and every matrix $\mathbf{B} \in U$, we have $\mathbf{BAB}^{-1} \in M$. Let $\mathbf{A} \in M$ and let $\mathbf{B} \in U$. Then

$$\mathbf{A} = \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$$

for some $x, y, r, s, u \in \mathbb{R}$ where $x \neq 0$ and $ru \neq 0$.

We have

$$\begin{aligned} \mathbf{BAB}^{-1} &= \begin{pmatrix} r & s \\ 0 & u \end{pmatrix} \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}^{-1} \\ &= \begin{pmatrix} rx & ry + sx \\ 0 & ux \end{pmatrix} \times \frac{1}{ru} \begin{pmatrix} u & -s \\ 0 & r \end{pmatrix} \\ &= \frac{1}{ru} \begin{pmatrix} rux & -rsx + r^2y + rsx \\ 0 & rux \end{pmatrix} \\ &= \begin{pmatrix} x & ry/u \\ 0 & x \end{pmatrix}. \end{aligned}$$

To check that $\mathbf{BAB}^{-1} \in M$, we have to check that it is of the form specified before the colon in the definition of M, namely

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix},$$

and also that it satisfies the conditions given after the colon, namely $a, b \in \mathbb{R}$, $a \neq 0$.

This matrix is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = x$ and $b = ry/u$. Also $x \neq 0$. Hence $\mathbf{BAB}^{-1} \in M$.

Thus M is a normal subgroup of U.

(b) Again we use Property B of Theorem E33.

This time we have to show that it is not satisfied.

We have to show that there is a matrix $\mathbf{A} \in M$ and a matrix $\mathbf{B} \in \mathrm{GL}(2)$ such that $\mathbf{BAB}^{-1} \notin M$.

To find such matrices, we can start with a general matrix $\mathbf{A} \in M$ and a general matrix $\mathbf{B} \in \mathrm{GL}(2)$ and proceed in a similar way to part (a) until things go wrong, as they must since M is not normal in $\mathrm{GL}(2)$. Looking at what has gone wrong can help us find suitable matrices. Alternatively, we can try finding suitable matrices by considered experimentation.

We have

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \in M \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2),$$

but

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}. \end{aligned}$$

This matrix is not in M since it is not an upper triangular matrix.

Hence M is not a normal subgroup of $\mathrm{GL}(2)$.

Here are two exercises about normal subgroups of matrix groups for you to try. You can use methods similar to those used in Worked Exercise E36.

Exercise E97

Determine whether the group D of all invertible 2×2 diagonal matrices, given by

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad \neq 0 \right\}$$

is a normal subgroup of GL(2).

Exercise E98

(a) Show that the set

$$S = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$$

is a subgroup of GL(2).

(b) Determine whether S is a normal subgroup of GL(2).

(c) Determine whether S is a normal subgroup of the group U of all invertible 2×2 upper triangular matrices.

In Worked Exercise E36 at the start of this subsection you saw that the set

$$M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\}$$

is a normal subgroup of the group U of all invertible 2×2 upper triangular matrices. It follows that the quotient group U/M exists. The elements of this quotient group are the cosets of M in U. It can be shown that for every coset of M in U there is one, and only one, non-zero real number x such that the coset can be expressed as

$$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} M.$$

So there is a one-to-one correspondence between the elements of the quotient group U/M and the elements of the set $\mathbb{R}^*$, given by

$$\begin{aligned} \phi : U/M &\longrightarrow \mathbb{R}^* \\ \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} M &\longmapsto x. \end{aligned}$$

In fact, it can be shown that this mapping ϕ is an isomorphism, so the quotient group U/M is isomorphic to the group $(\mathbb{R}^*, \times)$. There is a challenging exercise in the additional exercises booklet for this unit that asks you to prove this.

Summary

In this unit you studied two important topics that are both related to normal subgroups. First you saw that we can use a normal subgroup of a group to obtain a *quotient group*, a group whose elements are the cosets of the subgroup and whose binary operation is inherited from the binary operation of the group. You saw that in this way a normal subgroup of a group can be used to 'break down' the group into two simpler groups, just as a positive divisor of a natural number can be used to break down the number into two simpler numbers. You went on to study *conjugacy*. You saw what this means, and how we can interpret it in symmetric groups and in symmetry groups. You also saw (particularly in the context of matrix groups) that conjugacy provides convenient ways of checking whether a subgroup of a group is normal, and ways of finding new subgroups of a group when we already have some subgroups.

Learning outcomes

After working through this unit, you should be able to:

- explain what is meant by a *quotient group*
- construct the group table of a quotient group G/N where G is a fairly small finite group and N is a normal subgroup of G
- understand the structures of the quotient groups $\mathbb{Z}/n\mathbb{Z}$, where n is an integer with $n \geq 2$, and the quotient group $\mathbb{R}/\mathbb{Z}$
- explain the terms *conjugate* and *conjugacy class*
- state some properties of conjugate elements
- efficiently determine the conjugacy classes of a finite group of reasonably small order
- use conjugacy to test whether a subgroup of a group is a normal subgroup
- determine conjugate subgroups of a subgroup of a finite group
- use conjugacy classes to find normal subgroups of a group
- understand and use the features of conjugacy in symmetry groups
- use conjugacy in matrix groups to find conjugate subgroups and to determine whether a subgroup is a normal subgroup.

Solutions to exercises

Solution to Exercise E49

(a)
$$\begin{aligned}\{e,b\}\cdot\{r,t\} &= \{e\circ r,\ e\circ t,\ b\circ r,\ b\circ t\}\\ &= \{r,t,t,r\}\\ &= \{r,t\}\end{aligned}$$

(b)
$$\begin{aligned}\{a,c\}\cdot\{a,c\} &= \{a\circ a,\ a\circ c,\ c\circ a,\ c\circ c\}\\ &= \{b,e,e,b\}\\ &= \{e,b\}\end{aligned}$$

(c)
$$\begin{aligned}\{a,s\}\cdot\{a,s\} &= \{a\circ a,\ a\circ s,\ s\circ a,\ s\circ s\}\\ &= \{b,t,r,e\}\end{aligned}$$

(d)
$$\begin{aligned}&\{a,s\}\cdot\{a,s,e\}\\ &= \{a\circ a,\ a\circ s,\ a\circ e,\ s\circ a,\ s\circ s,\ s\circ e\}\\ &= \{b,t,a,r,e,s\}\end{aligned}$$

Solution to Exercise E50

(a)
$$\begin{aligned}&\{1,4,7\}+\{1,4,7\}\\ &= \{1+_9 1,\ 1+_9 4,\ 1+_9 7,\\ &\qquad 4+_9 1,\ 4+_9 4,\ 4+_9 7,\\ &\qquad 7+_9 1,\ 7+_9 4,\ 7+_9 7\}\\ &= \{2,5,8,5,8,2,8,2,5\}\\ &= \{2,5,8\}\end{aligned}$$

(b)
$$\begin{aligned}&\{0,3,6\}+\{1,4,7\}\\ &= \{0+_9 1,\ 0+_9 4,\ 0+_9 7,\\ &\qquad 3+_9 1,\ 3+_9 4,\ 3+_9 7,\\ &\qquad 6+_9 1,\ 6+_9 4,\ 6+_9 7\}\\ &= \{1,4,7,4,7,1,7,1,4\}\\ &= \{1,4,7\}\end{aligned}$$

Solution to Exercise E51

By the solution to Worked Exercise E19(b),

$$\{b,t\}\cdot\{c,u\} = \{a,s,u,c\}.$$

Also,

$$\begin{aligned}\{c,u\}\cdot\{b,t\} &= \{c\circ b,\ c\circ t,\ u\circ b,\ u\circ t\}\\ &= \{a,s,s,a\}\\ &= \{a,s\}.\end{aligned}$$

Thus

$$\{b,t\}\cdot\{c,u\} \neq \{c,u\}\cdot\{b,t\}.$$

Solution to Exercise E52

(a) The Cayley table for the cosets of the normal subgroup $\{e,b\}$ of $S(\square)$ under set composition is as follows.

$\cdot$	$\{e,b\}$	$\{a,c\}$	$\{r,t\}$	$\{s,u\}$
$\{e,b\}$	$\{e,b\}$	$\{a,c\}$	$\{r,t\}$	$\{s,u\}$
$\{a,c\}$	$\{a,c\}$	$\{e,b\}$	$\{s,u\}$	$\{r,t\}$
$\{r,t\}$	$\{r,t\}$	$\{s,u\}$	$\{e,b\}$	$\{a,c\}$
$\{s,u\}$	$\{s,u\}$	$\{r,t\}$	$\{a,c\}$	$\{e,b\}$

(b) All the sets in the body of the table are cosets of $\{e,b\}$ in $S(\square)$.

Solution to Exercise E53

(a) The Cayley table for the cosets of the normal subgroup $\{0,3,6\}$ of the group $\mathbb{Z}_9$ under set composition is as follows.

$+$	$\{0,3,6\}$	$\{1,4,7\}$	$\{2,5,8\}$
$\{0,3,6\}$	$\{0,3,6\}$	$\{1,4,7\}$	$\{2,5,8\}$
$\{1,4,7\}$	$\{1,4,7\}$	$\{2,5,8\}$	$\{0,3,6\}$
$\{2,5,8\}$	$\{2,5,8\}$	$\{0,3,6\}$	$\{1,4,7\}$

(b) All the sets in the body of the table are cosets of $\{0,3,6\}$ in $\mathbb{Z}_9$.

Solution to Exercise E54

We have, for example,

$$\{a,s\}\cdot\{c,u\} = \{e,r,t,b\}.$$

This example shows that composing two left cosets of the subgroup $\{e,r\}$ in the group $S(\square)$ does not necessarily give another left coset of $\{e,r\}$. Thus the set of left cosets of $\{e,r\}$ in $S(\square)$ is not closed under set composition.

Similarly, we have

$$\{a,u\}\cdot\{c,s\} = \{e,t,r,b\}.$$

This example shows that the set of right cosets of $\{e,r\}$ in $S(\square)$ is not closed under set composition in $S(\square)$.

(There are many other counterexamples.)

Solution to Exercise E55

(Remember that $\mathbb{Z}_{17}^* = \{1, 2, \ldots, 16\}$, and that the binary operation of the group $\mathbb{Z}_{17}^*$ is $\times_{17}$.)

(a) In $\mathbb{Z}_{17}^*$ we have

$$\begin{aligned}
&4^2 = 4 \times_{17} 4 = 16,\\
&4^3 = 4^2 \times_{17} 4 = 16 \times_{17} 4 = 13\\
&\quad (\text{since } 16 \times 4 \equiv (-1) \times 4 \equiv -4 \equiv 13 \pmod{17}),\\
&4^4 = 4^3 \times_{17} 4 = 13 \times_{17} 4 = 1\\
&\quad (\text{since } 13 \times 4 \equiv (-4) \times 4 \equiv -16 \equiv 1 \pmod{17}).
\end{aligned}$$

So 4 has order 4 and

$$N = \langle 4 \rangle = \{1, 4, 13, 16\}.$$

This subgroup of $\mathbb{Z}_{17}^*$ is normal in $\mathbb{Z}_{17}^*$ because $\mathbb{Z}_{17}^*$ is abelian.

(b) The cosets are

$$\begin{aligned}
N &= \{1, 4, 13, 16\},\\
2N &= \{2 \times_{17} 1,\ 2 \times_{17} 4,\ 2 \times_{17} 13,\ 2 \times_{17} 16\}\\
&= \{2, 8, 9, 15\},\\
3N &= \{3 \times_{17} 1,\ 3 \times_{17} 4,\ 3 \times_{17} 13,\ 3 \times_{17} 16\}\\
&= \{3, 12, 5, 14\}\\
&= \{3, 5, 12, 14\},\\
6N &= \{6 \times_{17} 1,\ 6 \times_{17} 4,\ 6 \times_{17} 13,\ 6 \times_{17} 16\}\\
&= \{6, 7, 10, 11\}.
\end{aligned}$$

(c) The group table of $\mathbb{Z}_{17}^*/N$ is as follows.

$\cdot$	N	$2N$	$3N$	$6N$
N	N	$2N$	$3N$	$6N$
$2N$	$2N$	N	$6N$	$3N$
$3N$	$3N$	$6N$	$2N$	N
$6N$	$6N$	$3N$	N	$2N$

(The rule for composing cosets of N in $\mathbb{Z}_{17}^*$ is

$$xN \cdot yN = (x \times_{17} y)N \quad \text{for all } x, y \in \mathbb{Z}_{17}^*.)$$

(d) The identity element of $\mathbb{Z}_{17}^*/N$ is N. The inverses of its elements are given below.

Element	N	$2N$	$3N$	$6N$
Inverse	N	$2N$	$6N$	$3N$

(e) The group $\mathbb{Z}_{17}^*/N$ has four elements, exactly two of which are self-inverse, so it is isomorphic to the cyclic group C_4.

Solution to Exercise E56

(Remember that $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$, and that the binary operation of the group $\mathbb{Z}_{12}$ is $+_{12}$.)

(a) In $\mathbb{Z}_{12}$ we have

$$2(6) = 6 +_{12} 6 = 0,$$

so 6 has order 2 and hence $H = \langle 6 \rangle = \{0, 6\}$. This subgroup of $\mathbb{Z}_{12}$ is normal in $\mathbb{Z}_{12}$ because $\mathbb{Z}_{12}$ is abelian.

(b) The cosets of H in $\mathbb{Z}_{12}$ are

$$\begin{aligned}
H &= \{0, 6\},\\
1 + H &= \{1, 7\},\\
2 + H &= \{2, 8\},\\
3 + H &= \{3, 9\},\\
4 + H &= \{4, 10\},\\
5 + H &= \{5, 11\}.
\end{aligned}$$

(c) The group table of $\mathbb{Z}_{12}/H$ is as follows.

$+$	H	$1+H$	$2+H$	$3+H$	$4+H$	$5+H$
H	H	$1+H$	$2+H$	$3+H$	$4+H$	$5+H$
$1+H$	$1+H$	$2+H$	$3+H$	$4+H$	$5+H$	H
$2+H$	$2+H$	$3+H$	$4+H$	$5+H$	H	$1+H$
$3+H$	$3+H$	$4+H$	$5+H$	H	$1+H$	$2+H$
$4+H$	$4+H$	$5+H$	H	$1+H$	$2+H$	$3+H$
$5+H$	$5+H$	H	$1+H$	$2+H$	$3+H$	$4+H$

(The rule for composing cosets of H in $\mathbb{Z}_{12}$ is

$$(x + H) + (y + H) = (x +_{12} y)H \quad \text{for all } x, y \in \mathbb{Z}_{12}.)$$

(d) The identity element of $\mathbb{Z}_{12}/H$ is H. The inverses of its elements are given below.

Element	H	$1+H$	$2+H$	$3+H$	$4+H$	$5+H$
Inverse	H	$5+H$	$4+H$	$3+H$	$2+H$	$1+H$

(e) The group $\mathbb{Z}_{12}/H$ is abelian and has six elements, so it is isomorphic to the cyclic group C_6.

Solution to Exercise E57

(a) The group table of G shows that $a^2 = e$, so N is the subgroup $\langle a\rangle$ of G generated by a. Also, the group table of G is symmetric with respect to the main diagonal, so G is abelian and hence N is normal in G.

(b) The cosets are

$$\begin{aligned} N &= \{e, a\},\\ bN &= \{be, ba\} = \{b, c\},\\ dN &= \{de, da\} = \{d, f\},\\ gN &= \{ge, ga\} = \{g, h\}. \end{aligned}$$

(c) The group table of G/N is as follows.

$\cdot$	N	bN	dN	gN
N	N	bN	dN	gN
bN	bN	N	gN	dN
dN	dN	gN	N	bN
gN	gN	dN	bN	N

(The rule for composing cosets of N in G is

$$xN \cdot yN = (xy)N \quad \text{for all } x, y \in G.)$$

(d) The identity element of G/N is N. Each element is self-inverse.

(e) The group G/N has four elements and each element is self-inverse, so it is isomorphic to the Klein four-group V.

(The quotient group G/N here can be spotted as a blocking of the given group table for G, as shown below.)

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	a	e	g	h	d	f
c	c	b	e	a	h	g	f	d
d	d	f	g	h	e	a	b	c
f	f	d	h	g	a	e	c	b
g	g	h	d	f	b	c	e	a
h	h	g	f	d	c	b	a	e

Solution to Exercise E58

(a) In G we have

$$\begin{aligned} r^2 &= s,\\ r^3 &= r^2 r = sr = e. \end{aligned}$$

So r has order 3 and

$$\langle r\rangle = \{e, r, s\} = N.$$

Thus N is a subgroup of G.

Also, N has index 2 in G, so it is normal in G.

(b) The cosets are

$$\begin{aligned} N &= \{e, r, s\},\\ pN &= \{p, q, t\}. \end{aligned}$$

(c) The group table of G/N is as follows.

$\cdot$	N	pN
N	N	pN
pN	pN	N

(The rule for composing cosets of N in G is

$$xN \cdot yN = (xy)N \quad \text{for all } x, y \in G.)$$

(d) The identity element of G/N is N. Each element is self-inverse.

(e) The group G/N has two elements, so it is isomorphic to the cyclic group C_2.

Solution to Exercise E59

The elements of $\mathbb{Z}/4\mathbb{Z}$ are the cosets of $4\mathbb{Z}$ in $\mathbb{Z}$.

The cosets are

$$\begin{aligned} 4\mathbb{Z} &= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\},\\ 1 + 4\mathbb{Z} &= \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\},\\ 2 + 4\mathbb{Z} &= \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\},\\ 3 + 4\mathbb{Z} &= \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}. \end{aligned}$$

Hence $\mathbb{Z}/4\mathbb{Z}$ has order 4.

Solution to Exercise E60

The group table of $\mathbb{Z}/4\mathbb{Z}$ is as follows.

$\boldsymbol{+}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

(For example,

$$\begin{aligned}
&(1+4\mathbb{Z}) \mathbin{\boldsymbol{+}} (2+4\mathbb{Z}) = 3+4\mathbb{Z},\\
&(3+4\mathbb{Z}) \mathbin{\boldsymbol{+}} (3+4\mathbb{Z}) = 6+4\mathbb{Z} = 2+4\mathbb{Z}\\
&\qquad\qquad\qquad\qquad\qquad\qquad (\text{since } 6 \in 2+4\mathbb{Z}),\\
&(1+4\mathbb{Z}) \mathbin{\boldsymbol{+}} (3+4\mathbb{Z}) = 4+4\mathbb{Z} = 4\mathbb{Z}\\
&\qquad\qquad\qquad\qquad\qquad\qquad (\text{since } 4 \in 4\mathbb{Z}).)
\end{aligned}$$

Solution to Exercise E61

A suitable isomorphism is

$$\begin{aligned}
\phi : \mathbb{Z}/4\mathbb{Z} &\longrightarrow \mathbb{Z}_4\\
a+4\mathbb{Z} &\longmapsto a, \quad \text{for } a = 0,1,2,3.
\end{aligned}$$

Solution to Exercise E62

(a) By Theorem E16, $\mathbb{Z}/6\mathbb{Z}$ is isomorphic to $\mathbb{Z}_6$ and an isomorphism is

$$\begin{aligned}
\phi : \mathbb{Z}/6\mathbb{Z} &\longrightarrow \mathbb{Z}_6\\
a+6\mathbb{Z} &\longmapsto a, \quad \text{for } a = 0,1,2,3,4,5.
\end{aligned}$$

The generators of $\mathbb{Z}_6$ are 1 and 5. These integers are the images under the isomorphism ϕ of the elements $1+6\mathbb{Z}$ and $5+6\mathbb{Z}$ of $\mathbb{Z}/6\mathbb{Z}$. Hence the generators of $\mathbb{Z}/6\mathbb{Z}$ are $1+6\mathbb{Z}$ and $5+6\mathbb{Z}$.

(b) The generators of $\mathbb{Z}_4$ are 1 and 3. So, by an argument similar to that in part (a), the generators of $\mathbb{Z}/4\mathbb{Z}$ are $1+4\mathbb{Z}$ and $3+4\mathbb{Z}$.

(c) The generators of $\mathbb{Z}_5$ are 1, 2, 3 and 4. So, by an argument similar to that in part (a), the generators of $\mathbb{Z}/5\mathbb{Z}$ are $1+5\mathbb{Z}$, $2+5\mathbb{Z}$, $3+5\mathbb{Z}$ and $4+5\mathbb{Z}$.

Solution to Exercise E63

(a) We have

$$\begin{aligned}
0.2+\mathbb{Z} &= \{\dots, -1.8, -0.8, 0.2, 1.2, 2.2, 3.2, \dots\},\\
1.2+\mathbb{Z} &= \{\dots, -0.8, 0.2, 1.2, 2.2, 3.2, 4.2, \dots\},\\
3.7+\mathbb{Z} &= \{\dots, 1.7, 2.7, 3.7, 4.7, 5.7, 6.7, \dots\},\\
-1.3+\mathbb{Z} &= \{\dots, -3.3, -2.3, -1.3,\\
&\qquad\qquad\qquad -0.3, 0.7, 1.7, \dots\},\\
-4.8+\mathbb{Z} &= \{\dots, -6.8, -5.8, -4.8,\\
&\qquad\qquad\qquad -3.8, -2.8, -1.8, \dots\}.
\end{aligned}$$

(b) There are only two different cosets in the list because

$$\begin{aligned}
&0.2+\mathbb{Z}\\
&\ = 1.2+\mathbb{Z}\\
&\ = -4.8+\mathbb{Z}\\
&\ = \{\dots, -2.8, -1.8, -0.8, 0.2, 1.2, 2.2, 3.2, \dots\},
\end{aligned}$$

and

$$\begin{aligned}
&3.7+\mathbb{Z}\\
&\ = -1.3+\mathbb{Z}\\
&\ = \{\dots, -2.3, -1.3, -0.3, 0.7, 1.7, 2.7, 3.7, \dots\}.
\end{aligned}$$

Solution to Exercise E64

(a) We have that $3.1 = 0.1 + 3$ and $0.1 \in [0,1)$, so

$$3.1+\mathbb{Z} = 0.1+\mathbb{Z}.$$

(b) We have that $-0.22 = 0.78 + (-1)$ and $0.78 \in [0,1)$, so

$$-0.22+\mathbb{Z} = 0.78+\mathbb{Z}.$$

(c) We have that $-3.1 = 0.9 + (-4)$ and $0.9 \in [0,1)$, so

$$-3.1+\mathbb{Z} = 0.9+\mathbb{Z}.$$

Solution to Exercise E65

(a) $$\begin{aligned}
(0.9+\mathbb{Z}) \mathbin{\boldsymbol{+}} (0.8+\mathbb{Z}) &= (0.9 +_1 0.8) + \mathbb{Z}\\
&= 0.7+\mathbb{Z}
\end{aligned}$$

(b) $$\begin{aligned}
(0.2+\mathbb{Z}) \mathbin{\boldsymbol{+}} \mathbb{Z} &= (0.2+\mathbb{Z}) \mathbin{\boldsymbol{+}} (0+\mathbb{Z})\\
&= (0.2 +_1 0) + \mathbb{Z}\\
&= 0.2+\mathbb{Z}
\end{aligned}$$

(c) $(0.5+\mathbb{Z})+(0.7+\mathbb{Z})+(0.8+\mathbb{Z})$

$$\begin{aligned} &= (0.5 +_1 0.7 +_1 0.8) + \mathbb{Z} \\ &= 0 + \mathbb{Z} \\ &= \mathbb{Z} \end{aligned}$$

Solution to Exercise E66

(a) The element $0.25+\mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$ maps to the element 0.25 of the group $([0,1),+_1)$ under the isomorphism in Theorem E17. So these two elements have the same order.

The element 0.25 of the group $([0,1),+_1)$ has order 4, because

$$\begin{aligned} 2(0.25) &= 0.25 +_1 0.25 = 0.5, \\ 3(0.25) &= 2(0.25) +_1 0.25 = 0.5 +_1 0.25 = 0.75, \\ 4(0.25) &= 3(0.25) +_1 0.25 = 0.75 +_1 0.25 = 0. \end{aligned}$$

It follows that the element $0.25+\mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$ also has order 4.

The cyclic subgroup generated by this element is

$$\{\mathbb{Z},\ 0.25+\mathbb{Z},\ 0.5+\mathbb{Z},\ 0.75+\mathbb{Z}\}.$$

(b) We can obtain elements with the specified orders by using the ideas of part (a).

(i) An element of $\mathbb{R}/\mathbb{Z}$ of order 5 is $0.2+\mathbb{Z}$.

(ii) An element of $\mathbb{R}/\mathbb{Z}$ of order 2 is $0.5+\mathbb{Z}$.

(iii) An element of $\mathbb{R}/\mathbb{Z}$ of order 3 is $\frac{1}{3}+\mathbb{Z}$.

(iv) An element of $\mathbb{R}/\mathbb{Z}$ of order 1 is the identity element $\mathbb{Z}$.

Solution to Exercise E67

(a) The group $S(\square)$ is not simple. The set $S^+(\square)$ of direct symmetries in $S(\square)$ is a subgroup of $S(\square)$ (by Theorem B25, which you revised in Subsection 1.4 of Unit E1), and it is normal in $S(\square)$ since it has index 2 (see Theorem E11 in Unit E1).

(b) The group $\mathbb{Z}_6$ is not simple. By Theorem B41 (which you revised in Subsection 3.3 of Unit E1), the subgroups of $\mathbb{Z}_6$ are cyclic subgroups of orders 1, 2, 3 and 6 and, since $\mathbb{Z}_6$ is abelian, these subgroups are all normal by Theorem E10 in Unit E1.

(c) The group $\mathbb{Z}_7$ is simple. By Theorem B41, the only subgroups of $\mathbb{Z}_7$ are cyclic subgroups of orders 1 and 7. Thus the only normal subgroups of $\mathbb{Z}_7$ are the trivial subgroup $\{0\}$ and $\mathbb{Z}_7$.

Solution to Exercise E68

(a) **(i)** We use the conjugating permutation $(1\ 3\ 5)$ to rename the symbols in $(1\ 2\ 4\ 3\ 5)$:

$$\begin{array}{cl} & (1\ 2\ 4\ 3\ 5) \\ (1\ 3\ 5) & \ \downarrow\downarrow\downarrow\downarrow\downarrow \\ & (3\ 2\ 4\ 5\ 1) = (1\ 3\ 2\ 4\ 5). \end{array}$$

Thus

$$(1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (1\ 3\ 5)^{-1} = (1\ 3\ 2\ 4\ 5).$$

(ii) Using the renaming method, we obtain

$$\begin{array}{cl} & (1\ 5\ 2) \\ (1\ 3)(2\ 4\ 5) & \ \downarrow\downarrow\downarrow \\ & (3\ 2\ 4) = (2\ 4\ 3). \end{array}$$

Thus

$$(1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ \big((1\ 3)(2\ 4\ 5)\big)^{-1} = (2\ 4\ 3).$$

(b) We can check the answers to part (a) as follows.

(i) $(1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (1\ 3\ 5)^{-1}$

$$\begin{aligned} &= (1\ 3\ 5) \circ (1\ 2\ 4\ 3\ 5) \circ (5\ 3\ 1) \\ &= (1\ 3\ 2\ 4\ 5) \end{aligned}$$

(ii) $(1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ \big((1\ 3)(2\ 4\ 5)\big)^{-1}$

$$\begin{aligned} &= (1\ 3)(2\ 4\ 5) \circ (1\ 5\ 2) \circ (3\ 1)(5\ 4\ 2) \\ &= (1)(2\ 4\ 3)(5) \\ &= (2\ 4\ 3) \end{aligned}$$

Solution to Exercise E69

The permutation $(2\ 3\ 5)(4\ 6)$ can be written in the form $(-\ -\ -)(-\ -)$ in six different ways:

$$\begin{array}{ll} (2\ 3\ 5)(4\ 6), & (2\ 3\ 5)(6\ 4), \\ (3\ 5\ 2)(4\ 6), & (3\ 5\ 2)(6\ 4), \\ (5\ 2\ 3)(4\ 6), & (5\ 2\ 3)(6\ 4). \end{array}$$

The conjugating permutation in Worked Exercise E24 corresponds to the middle way in the left-hand column above, and the two conjugating permutations in Worked Exercise E25 correspond to the other two ways in the left-hand column.

So we can obtain three more conjugating permutations by writing $(2\ 3\ 5)(4\ 6)$ in the three ways in the right-hand column. We obtain:

$$g\ \begin{array}{l}(1\ 4\ 3)(2\ 6)(5)\\ \ \downarrow\,\downarrow\,\downarrow\ \ \downarrow\,\downarrow\ \ \downarrow\\ (2\ 3\ 5)(6\ 4)(1)\end{array}, \text{ which gives } g=(1\ 2\ 6\ 4\ 3\ 5);$$

$$g\ \begin{array}{l}(1\ 4\ 3)(2\ 6)(5)\\ \ \downarrow\,\downarrow\,\downarrow\ \ \downarrow\,\downarrow\ \ \downarrow\\ (3\ 5\ 2)(6\ 4)(1)\end{array}, \text{ which gives } g=(1\ 3\ 2\ 6\ 4\ 5);$$

$$g\ \begin{array}{l}(1\ 4\ 3)(2\ 6)(5)\\ \ \downarrow\,\downarrow\,\downarrow\ \ \downarrow\,\downarrow\ \ \downarrow\\ (5\ 2\ 3)(6\ 4)(1)\end{array}, \text{ which gives } g=(1\ 5)(2\ 6\ 4).$$

So the other three permutations in S_6 that conjugate $(1\ 4\ 3)(2\ 6)$ to $(2\ 3\ 5)(4\ 6)$ are $(1\ 2\ 6\ 4\ 3\ 5)$, $(1\ 3\ 2\ 6\ 4\ 5)$ and $(1\ 5)(2\ 6\ 4)$.

Solution to Exercise E70

There are four ways to match up the cycles, as follows:

$$g\ \begin{array}{l}(1\ 3)(2)(4)\\ \ \downarrow\,\downarrow\ \ \downarrow\ \ \downarrow\\ (3\ 4)(1)(2)\end{array}, \text{ which gives } g=(1\ 3\ 4\ 2);$$

$$g\ \begin{array}{l}(1\ 3)(2)(4)\\ \ \downarrow\,\downarrow\ \ \downarrow\ \ \downarrow\\ (3\ 4)(2)(1)\end{array}, \text{ which gives } g=(1\ 3\ 4);$$

$$g\ \begin{array}{l}(1\ 3)(2)(4)\\ \ \downarrow\,\downarrow\ \ \downarrow\ \ \downarrow\\ (4\ 3)(1)(2)\end{array}, \text{ which gives } g=(1\ 4\ 2);$$

$$g\ \begin{array}{l}(1\ 3)(2)(4)\\ \ \downarrow\,\downarrow\ \ \downarrow\ \ \downarrow\\ (4\ 3)(2)(1)\end{array}, \text{ which gives } g=(1\ 4).$$

So the permutations in S_4 that conjugate $(1\ 3)$ to $(3\ 4)$ are $(1\ 3\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 2)$ and $(1\ 4)$.

Solution to Exercise E71

(a) $s \circ a \circ s^{-1} = s \circ (a \circ s) = s \circ r = b$

(b) $a \circ a \circ a^{-1} = a \circ (a \circ b) = a \circ e = a$

(c) $e \circ a \circ e^{-1} = e \circ (a \circ e) = e \circ a = a$

(d) $b \circ a \circ b^{-1} = b \circ (a \circ a) = b \circ b = a$

Solution to Exercise E72

Let g be any element of G. Then, since G is abelian,

$$gxg^{-1} = xgg^{-1} = xe = x,$$

as required.

Solution to Exercise E73

(a) $xex^{-1} = xx^{-1} = e$

(b) $exe^{-1} = exe = ex = x$

Solution to Exercise E74

(a) Since $y = gxg^{-1}$, we have

$$\begin{aligned} y^2 &= gxg^{-1}gxg^{-1}\\ &= gxexg^{-1}\\ &= gx^2g^{-1}. \end{aligned}$$

(b) Since $y = gxg^{-1}$ and, by part (a), $y^2 = gx^2g^{-1}$, we have

$$\begin{aligned} y^3 &= y^2y\\ &= gx^2g^{-1}gxg^{-1}\\ &= gx^2exg^{-1}\\ &= gx^3g^{-1}. \end{aligned}$$

(c) Since $y = gxg^{-1}$ and, by part (b), $y^3 = gx^3g^{-1}$, we have

$$\begin{aligned} y^4 &= y^3y\\ &= gx^3g^{-1}gxg^{-1}\\ &= gx^3exg^{-1}\\ &= gx^4g^{-1}. \end{aligned}$$

Solution to Exercise E75

The group $\mathbb{Z}_6$ is abelian, so each element is conjugate to itself alone. Thus any two elements of the same order have the required property.

The orders of the elements of $\mathbb{Z}_6$ are as follows.

Element	0	1	2	3	4	5
Order	1	6	3	2	3	6

The elements 1 and 5 have the same order but are not conjugate.

Similarly, the elements 2 and 4 have the same order but are not conjugate.

Solution to Exercise E76

(a) The conjugates of c in $S(\square)$ are

$$\begin{aligned}
&e \circ c \circ e^{-1} = e \circ (c \circ e) = e \circ c = c,\\
&a \circ c \circ a^{-1} = a \circ (c \circ c) = a \circ b = c,\\
&b \circ c \circ b^{-1} = b \circ (c \circ b) = b \circ a = c,\\
&c \circ c \circ c^{-1} = c \circ e = c,\\
&r \circ c \circ r^{-1} = r \circ (c \circ r) = r \circ u = a,\\
&s \circ c \circ s^{-1} = s \circ (c \circ s) = s \circ r = a,\\
&t \circ c \circ t^{-1} = t \circ (c \circ t) = t \circ s = a,\\
&u \circ c \circ u^{-1} = u \circ (c \circ u) = u \circ t = a.
\end{aligned}$$

The conjugacy class of c in $S(\square)$ is $\{a, c\}$.

(b) In any group, conjugating the identity element e by any other element g just gives the identity element again: $geg^{-1} = gg^{-1} = e$, as you saw in Exercise E73(a). Therefore the conjugacy class of e in $S(\square)$ is $\{e\}$.

Solution to Exercise E77

The partition of $S(\triangle)$ by the orders of its elements is

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

The set $\{e\}$ is a conjugacy class.

Consider the set $\{a, b\}$. We have

$$r \circ a \circ r^{-1} = r \circ (a \circ r) = r \circ t = b.$$

Hence $\{a, b\}$ is a conjugacy class.

Now consider the set $\{r, s, t\}$. Conjugating r by e gives r. Also,

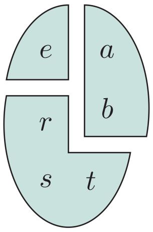
$$\begin{aligned}
&a \circ r \circ a^{-1} = a \circ (r \circ b) = a \circ t = s,\\
&b \circ r \circ b^{-1} = b \circ (r \circ a) = b \circ s = t.
\end{aligned}$$

Hence $\{r, s, t\}$ is a conjugacy class.

In summary, the conjugacy classes of $S(\triangle)$ are

$$\{e\}, \quad \{a, b\}, \quad \{r, s, t\}.$$

(The partition of $S(\triangle)$ into conjugacy classes is illustrated below.)



Solution to Exercise E78

We have $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.

Now $\mathbb{Z}_7^*$ is abelian and therefore each element of $\mathbb{Z}_7^*$ is conjugate only to itself, by the result proved in Exercise E72.

Hence the partition of $\mathbb{Z}_7^*$ into conjugacy classes is

$$\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}.$$

(Each conjugacy class contains a single element.)

Solution to Exercise E79

The group H has order 4 and is therefore abelian. So each element of H is conjugate only to itself in H.

However, all the non-identity elements of H have the same cycle structure and are therefore all conjugate to each other in S_4.

Solution to Exercise E80

Let G be a group with identity element e. We use Theorem E28 to show that $\{e\}$ and G are normal in G.

First consider the subgroup $\{e\}$. Let h be any element of $\{e\}$, that is, $h = e$, and let g be any element of G. Then

$$ghg^{-1} = geg^{-1} = gg^{-1} = e \in \{e\}.$$

Therefore $\{e\}$ is normal in G.

Next consider the subgroup G. Let h be any element of the subgroup G and let g be any element of the group G. Then, since g, h and g^{-1} all belong to G, we have $ghg^{-1} \in G$.

Therefore G is normal in G.

Solution to Exercise E81

Let H and K be normal subgroups of a group G. Then $H \cap K$ is a subgroup of G, by Theorem B81. We use Theorem E28 to show that $H \cap K$ is normal in G.

Let x be any element of $H \cap K$ and let g be any element of G. Then x is an element of H and also an element of K, so, since both H and K are normal in G,

$$gxg^{-1} \in H \quad \text{and} \quad gxg^{-1} \in K.$$

Hence

$$gxg^{-1} \in H \cap K.$$

Therefore $H \cap K$ is normal in G.

Solution to Exercise E82

(a) **(i)** Let $(a,b) \in X$. Then

$$(a,b) * (1,0) = (a \times 1, a \times 0 + b) = (a,b).$$

(ii) Let $(a,b) \in X$. Then

$$\begin{aligned}&\left(\frac{1}{a}, -\frac{b}{a}\right) * (a,b)\\ &= \left(\frac{1}{a} \times a,\ \frac{1}{a} \times b + \left(-\frac{b}{a}\right)\right)\\ &= (1,0).\end{aligned}$$

(b) **(i)** $(3,2) * (1,7) * (3,2)^{-1}$

$$\begin{aligned}&= ((3,2) * (1,7)) * \left(\tfrac{1}{3}, -\tfrac{2}{3}\right)\\ &= (3,23) * \left(\tfrac{1}{3}, -\tfrac{2}{3}\right)\\ &= (1,21)\end{aligned}$$

(ii) $(-1,3) * (1,-2) * (-1,3)^{-1}$

$$\begin{aligned}&= ((-1,3) * (1,-2)) * (-1,3)\\ &= (-1,5) * (-1,3)\\ &= (1,2)\end{aligned}$$

(c) Let $(1,b)$ be any element of A and let (c,d) be any element of X. Then $b,c,d \in \mathbb{R}$ and $c \neq 0$. We have to show that

$$(c,d) * (1,b) * (c,d)^{-1} \in A.$$

Now $(c,d)^{-1} = \left(\dfrac{1}{c}, -\dfrac{d}{c}\right)$, so we have

$$\begin{aligned}&(c,d) * (1,b) * (c,d)^{-1}\\ &= ((c,d) * (1,b)) * \left(\frac{1}{c}, -\frac{d}{c}\right)\\ &= (c, cb+d) * \left(\frac{1}{c}, -\frac{d}{c}\right)\\ &= (1, -d + cb + d)\\ &= (1, cb).\end{aligned}$$

The element $(1,cb)$ belongs to A, since its first coordinate is 1 (and $cb \in \mathbb{R}$). Thus, by Theorem E28, A is a normal subgroup of X.

(Note that part (b) provides supporting evidence that the subgroup A is normal in X: it gives two examples of conjugates of elements of A by elements of X, both of which turn out to be elements of A.)

Solution to Exercise E83

(a) We have, for example, $(1\ 2) \in H$ and $(1\ 3) \in S_4$, but

$$\begin{aligned}(1\ 3) \circ (1\ 2) \circ (1\ 3)^{-1} &= (3\ 2)\\ &= (2\ 3) \notin H.\end{aligned}$$

Therefore by Theorem E28 the subgroup H is not normal in S_4.

(b) We have, for example, $(1\ 3) \in H$ and $(1\ 2) \in S_4$, but

$$(1\ 2) \circ (1\ 3) \circ (1\ 2)^{-1} = (2\ 3) \notin H.$$

Therefore by Theorem E28 the subgroup H is not normal in S_4.

(The conjugates above can be found by using the renaming method.)

Solution to Exercise E84

First we show that K is a subgroup of X. We show that the three subgroup properties hold. (You revised these in Subsection 1.4 of Unit E1.)

SG1 Let $(1,m), (1,n) \in K$. Then $m,n \in \mathbb{Z}$. We have

$$(1,m) * (1,n) = (1, n+m).$$

This point has first coordinate 1 and its second coordinate $n+m$ is in $\mathbb{Z}$ because $m,n \in \mathbb{Z}$. Hence it is an element of K. Thus K is closed under $*$.

SG2 The identity element of X is $(1,0)$. This point has first coordinate 1, so it is an element of K.

SG3 Let $(1, n) \in K$. Then $n \in \mathbb{Z}$. The inverse of $(1, n)$ in X is $(1, -n)$. This point has first coordinate 1 and its second coordinate $-n$ is in $\mathbb{Z}$ because $n \in \mathbb{Z}$. Hence it is an element of K. Thus K contains the inverse of each of its elements.

Hence K satisfies the three subgroup properties and so is a subgroup of X.

To investigate whether K is normal in X, we determine the conjugate of a general element of K by a general element of X.

Let $(1, n) \in K$ and let $(a, b) \in X$. Then $n \in \mathbb{Z}$, and $a, b \in \mathbb{R}$ with $a \neq 0$. We have

$$\begin{aligned}
&(a, b) * (1, n) * (a, b)^{-1} \\
&= ((a, b) * (1, n)) * \left(\frac{1}{a}, -\frac{b}{a}\right) \\
&= (a, an + b) * \left(\frac{1}{a}, -\frac{b}{a}\right) \\
&= (1, -b + an + b) \\
&= (1, an).
\end{aligned}$$

We need to determine whether this point is always an element of K. It has first coordinate 1, so to check whether it is in K we need to check whether an is always an integer. However a need not be an integer, so an will not always be an integer: for example, if $a = \frac{1}{2}$ and $n = 3$, then $an = \frac{3}{2}$. Thus $(1, an)$ will not always be in K.

So we can now give a counterexample to demonstrate that K is not a normal subgroup of X. We have $(1, 3) \in K$ and $\left(\frac{1}{2}, 0\right) \in X$, but

$$\left(\tfrac{1}{2}, 0\right) * (1, 3) * \left(\tfrac{1}{2}, 0\right)^{-1} = \left(1, \tfrac{3}{2}\right) \notin K.$$

Therefore by Theorem E28 the subgroup K is not normal in X.

Solution to Exercise E85

From the group table for $S(\square)$ we obtain the following.

(a)
$$\begin{aligned}
aHa^{-1} &= \{a \circ e \circ a^{-1},\ a \circ s \circ a^{-1}\} \\
&= \{e,\ a \circ (s \circ c)\} \\
&= \{e,\ a \circ t\} \\
&= \{e, u\}
\end{aligned}$$

(b)
$$\begin{aligned}
rHr^{-1} &= \{r \circ e \circ r^{-1},\ r \circ b \circ r^{-1},\ r \circ s \circ r^{-1}, \\
&\qquad r \circ u \circ r^{-1}\} \\
&= \{e,\ r \circ (b \circ r),\ r \circ (s \circ r),\ r \circ (u \circ r)\} \\
&= \{e,\ r \circ t,\ r \circ a,\ r \circ c\} \\
&= \{e, b, u, s\} \\
&= H
\end{aligned}$$

Solution to Exercise E86

(a) **(i)** To determine $(1\ 2\ 4)K(1\ 2\ 4)^{-1}$, we use $(1\ 2\ 4)$ to rename the symbols in each element of K.

For example, we have

$$\begin{array}{ll}
 & (1\ 2)(3\ 4) \\
(1\ 2\ 4) & \ \downarrow\downarrow\ \ \downarrow\downarrow \\
 & (2\ 4)(3\ 1) = (1\ 3)(2\ 4),
\end{array}$$

so the conjugate of $(1\ 2)(3\ 4)$ by $(1\ 2\ 4)$ is $(1\ 3)(2\ 4)$.

This method gives

$$\begin{aligned}
&(1\ 2\ 4)K(1\ 2\ 4)^{-1} \\
&= \{e,\ (2\ 4)(3\ 1),\ (2\ 3)(4\ 1),\ (2\ 1)(4\ 3)\} \\
&= \{e,\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 2)(3\ 4)\}.
\end{aligned}$$

(Notice that $(1\ 2\ 4)K(1\ 2\ 4)^{-1} = K$.)

(ii) Similarly, using $(2\ 4\ 3)$ to rename the symbols in each element of K, we obtain

$$\begin{aligned}
&(2\ 4\ 3)K(2\ 4\ 3)^{-1} \\
&= \{e,\ (1\ 4)(2\ 3),\ (1\ 2)(4\ 3),\ (1\ 3)(4\ 2)\}.
\end{aligned}$$

(Notice that again $(2\ 4\ 3)K(2\ 4\ 3)^{-1} = K$.)

(b) Since conjugation does not change cycle structure, every conjugate subgroup gKg^{-1} of K in A_4 is a subgroup of A_4 of order 4 whose elements are the identity and three permutations all with cycle structure $(-\ -)(-\ -)$. However (as shown in Subsection 3.3 of Unit B3) there are only three permutations with this cycle structure in A_4, namely the three non-identity permutations in the subgroup K. It follows that every conjugate subgroup gKg^{-1} of K in A_4 is equal to K. So K has just one conjugate subgroup, namely itself.

Solution to Exercise E87

By the solution to Exercise E77, the conjugacy classes of $S(\triangle)$ are

$$\{e\}, \quad \{a,b\}, \quad \{r,s,t\}.$$

The following subgroups of $S(\triangle)$ are unions of conjugacy classes:

$$\{e\} = \{e\},$$
$$\{e,a,b\} = \{e\} \cup \{a,b\},$$
$$S(\triangle) = \{e\} \cup \{a,b\} \cup \{r,s,t\}.$$

Hence by Theorem E32 these three subgroups are normal subgroups of $S(\triangle)$.

The remaining three subgroups $\{e,r\}$, $\{e,s\}$ and $\{e,t\}$ of $S(\triangle)$ are not normal, since none of them can be expressed as a union of conjugacy classes.

Solution to Exercise E88

We apply Strategy E5.

We are given that A_5 has five conjugacy classes, and the numbers of elements in these classes are 1, 12, 12, 15 and 20.

We need to find all the unions of conjugacy classes that include the class $\{e\}$ and whose total number of elements is a divisor of $|A_5| = \frac{1}{2} \times 5! = 60$.

So we seek ways of adding some of the numbers

$$1,\ 12,\ 12,\ 15,\ 20,$$

always including 1, to obtain a total that is one of the numbers 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 or 60.

We can achieve the total 1 by taking the number 1 alone.

The smallest total greater than 1 that can be achieved with the given numbers, including 1, is $1 + 12 = 13$, so none of the totals 2, 3, 4, 5, 6, 10 and 12 is possible.

The smallest total greater than 13 that can be achieved is $1 + 15 = 16$, so the total 15 is not possible.

Since only one of the numbers other than 1 is odd, namely 15, any even total must include both the numbers 1 and 15. The smallest such totals that can be achieved are $1 + 15 = 16$, $1 + 15 + 12 = 28$ and $1 + 15 + 20 = 36$, so neither of the totals 20 and 30 is possible.

We can achieve the total 60 by adding all of the numbers.

Thus the only suitable sums of numbers are

$$1 \quad \text{and} \quad 1 + 12 + 12 + 15 + 20.$$

So the only unions of conjugacy classes that include $A = \{e\}$ and have a permissible number of elements are as follows:

$$A \qquad \text{(1 element)},$$
$$A \cup B \cup C \cup D \cup E \qquad \text{(60 elements)}.$$

If either of these sets is a subgroup, then it is a normal subgroup, by Theorem E32.

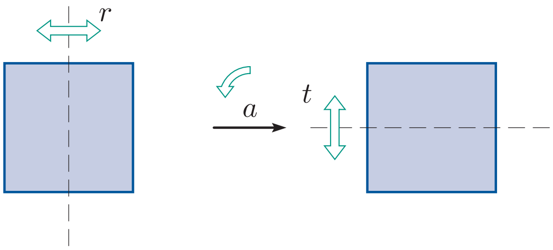
These sets are the set $\{e\}$ and the whole set A_5 respectively, so both are subgroups.

We conclude that the only normal subgroups of A_5 are the trivial subgroup $\{e\}$ and the whole group A_5.

(The solution to this exercise shows that A_5 is a *simple* group. The definition of a simple group was given in the optional Subsection 1.3.)

Solution to Exercise E89

(a) The symmetry a transforms a diagram illustrating the symmetry r into a diagram illustrating the symmetry t, as shown below.



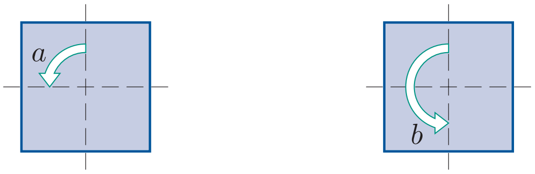
So the symmetry a conjugates r to t, that is,

$$t = a \circ r \circ a^{-1}.$$

Thus the symmetries r and t are conjugate in $S(\square)$.

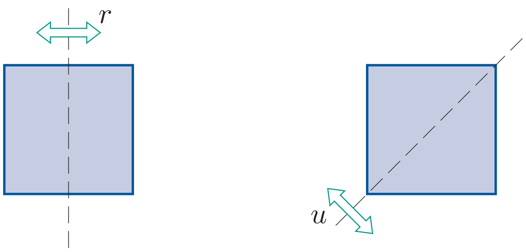
(Each of the symmetries c, s and u also transforms a diagram illustrating r into a diagram illustrating t and hence also conjugates r to t.)

(b) The symmetries a and b are shown below. There is no symmetry of the square that transforms a diagram illustrating a into a diagram illustrating b.



So there is no symmetry of the square that conjugates a to b and hence these symmetries are not conjugate in $S(\square)$.

(c) The symmetries r and u are shown below. There is no symmetry of the square that transforms a diagram illustrating r into a diagram illustrating u.

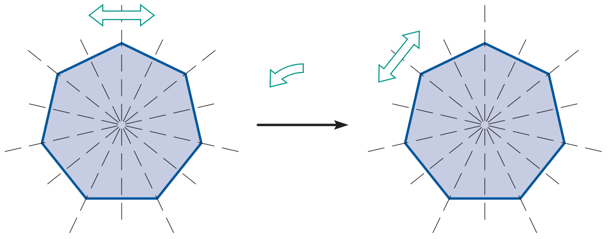


So there is no symmetry of the square that conjugates r to u and hence these symmetries are not conjugate in $S(\square)$.

Solution to Exercise E90

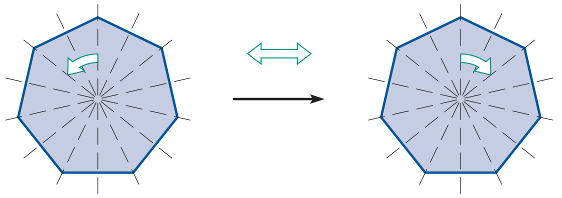
(a) Reflection in the vertical axis and reflection in the axis obtained by rotating the vertical axis by $2\pi/7$ anticlockwise are conjugate in S(heptagon).

A conjugating symmetry is rotation through $2\pi/7$ anticlockwise (or reflection in the axis obtained by rotating the vertical axis by $\pi/7$ anticlockwise).



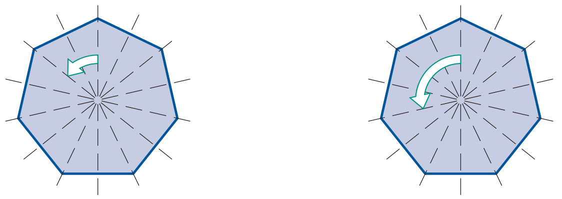
(b) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $12\pi/7$ (which is the same as clockwise rotation through $2\pi/7$) are conjugate in S(heptagon).

A conjugating symmetry is reflection in the vertical axis (or any reflection).



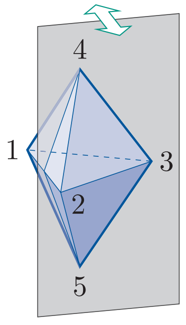
(c) Anticlockwise rotation through $2\pi/7$ and anticlockwise rotation through $4\pi/7$ are not conjugate in S(heptagon).

There is no symmetry of the heptagon that transforms a diagram illustrating the first of these symmetries into a diagram illustrating the second.



Solution to Exercise E91

(a) The fixed point set of the reflection in the plane through vertices 3, 4 and 5 is the portion of this plane that lies within the double tetrahedron, as shown below.

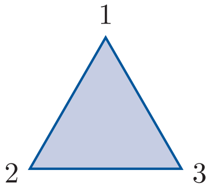


(b) The fixed point set of the reflection in the plane through vertices 1, 2 and 3 is the triangle with vertices 1, 2 and 3.

(c) The fixed point set of the rotation (1 2 3) is the line segment that joins vertices 4 and 5.

Solution to Exercise E92

The labelled triangle is as follows (repeated here for convenience).



(a) The symmetries of the triangle are as follows.

Rotations	Reflections
e	$(1\ 2)$
$(1\ 2\ 3)$	$(1\ 3)$
$(1\ 3\ 2)$	$(2\ 3)$

(b) The partition of $S(\triangle)$ by cycle structure is as follows.

$\{e\}$

$\{(1\ 2\ 3), (1\ 3\ 2)\}$

$\{(1\ 2), (1\ 3), (2\ 3)\}$

One conjugacy class is $\{e\}$.

Now consider the cycle structure class

$$\{(1\ 2\ 3), (1\ 3\ 2)\}.$$

The symmetries $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are rotations through $2\pi/3$ anticlockwise and $2\pi/3$ clockwise, respectively. Hence any reflection conjugates one to the other. Thus this cycle structure class is a conjugacy class.

Now consider the cycle structure class

$$\{(1\ 2), (1\ 3), (2\ 3)\}.$$

The symmetry $(1\ 2\ 3)$ (rotation through $2\pi/3$ anticlockwise) transforms a diagram illustrating the symmetry $(1\ 2)$ into a diagram illustrating the symmetry $(2\ 3)$.

Also, the symmetry $(1\ 3\ 2)$ (rotation through $4\pi/3$ anticlockwise) transforms a diagram illustrating the symmetry $(1\ 2)$ to a diagram illustrating the symmetry $(1\ 3)$.

Hence the three symmetries in this cycle structure class are all conjugate to each other. Thus this cycle structure class is also a conjugacy class.

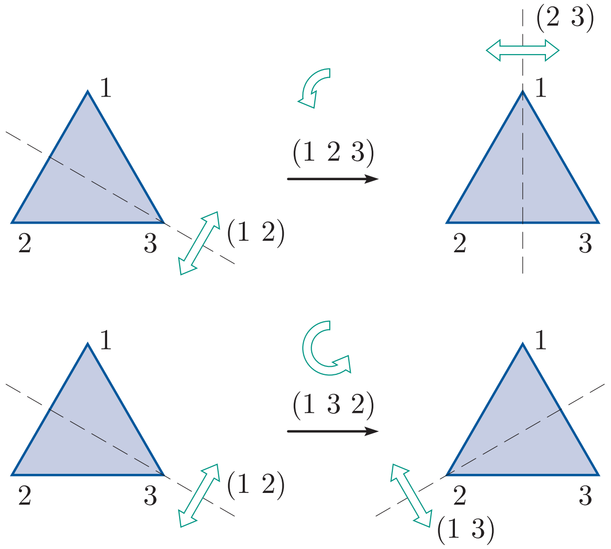
In summary, the conjugacy classes of $S(\triangle)$ are as follows.

$\{e\}$

$\{(1\ 2\ 3), (1\ 3\ 2)\}$

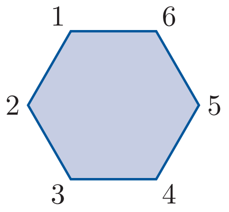
$\{(1\ 2), (1\ 3), (2\ 3)\}$

(The effects of the symmetries $(1\ 2\ 3)$ and $(1\ 3\ 2)$ mentioned above are shown below.)



Solution to Exercise E93

The labelled hexagon is as follows (repeated here for convenience).



(a) The symmetries of the hexagon are as follows.

Rotations	Reflections
e	$(1\ 6)(2\ 5)(3\ 4)$
$(1\ 2\ 3\ 4\ 5\ 6)$	$(1\ 2)(3\ 6)(4\ 5)$
$(1\ 3\ 5)(2\ 4\ 6)$	$(1\ 4)(2\ 3)(5\ 6)$
$(1\ 4)(2\ 5)(3\ 6)$	$(2\ 6)(3\ 5)$
$(1\ 5\ 3)(2\ 6\ 4)$	$(1\ 3)(4\ 6)$
$(1\ 6\ 5\ 4\ 3\ 2)$	$(1\ 5)(2\ 4)$

(You also met the symmetries of the hexagon expressed as permutations of the vertex labels earlier in the module, in Exercise B100 in Subsection 2.4 of Unit B3.)

(b) The partition of $S(\hexagon)$ by cycle structure is as follows.

$$\{e\}$$
$$\{(1\ 2\ 3\ 4\ 5\ 6),\ (1\ 6\ 5\ 4\ 3\ 2)\}$$
$$\{(1\ 3\ 5)(2\ 4\ 6),\ (1\ 5\ 3)(2\ 6\ 4)\}$$
$$\{(1\ 4)(2\ 5)(3\ 6),\ (1\ 6)(2\ 5)(3\ 4),\ (1\ 2)(3\ 6)(4\ 5),\ (1\ 4)(2\ 3)(5\ 6)\}$$
$$\{(2\ 6)(3\ 5),\ (1\ 3)(4\ 6),\ (1\ 5)(2\ 4)\}$$

One conjugacy class is $\{e\}$.

Now consider the cycle structure class

$$\{(1\ 2\ 3\ 4\ 5\ 6),\ (1\ 6\ 5\ 4\ 3\ 2)\}.$$

The two symmetries in this class are rotations through $\pi/3$ anticlockwise and $\pi/3$ clockwise, respectively. Hence any reflection conjugates one to the other. Thus this cycle structure class is a conjugacy class.

Next consider the cycle structure class

$$\{(1\ 3\ 5)(2\ 4\ 6),\ (1\ 5\ 3)(2\ 6\ 4)\}.$$

The two symmetries in this class are rotations through $2\pi/3$ anticlockwise and $2\pi/3$ clockwise, respectively. Hence any reflection conjugates one to the other. Thus this cycle structure class is a conjugacy class.

Next consider the cycle structure class

$$\{(1\ 4)(2\ 5)(3\ 6),\ (1\ 6)(2\ 5)(3\ 4),\ (1\ 2)(3\ 6)(4\ 5),\ (1\ 4)(2\ 3)(5\ 6)\}.$$

The symmetry $(1\ 4)(2\ 5)(3\ 6)$ is not conjugate to the other three symmetries here, because it is direct whereas the other three are indirect.

The three symmetries $(1\ 6)(2\ 5)(3\ 4)$, $(1\ 2)(3\ 6)(4\ 5)$ and $(1\ 4)(2\ 3)(5\ 6)$ are all reflections in axes that pass through two midpoints of edges. Hence for any pair of these symmetries there is a rotation of the hexagon that transforms a diagram illustrating one of the pair to a diagram illustrating the other. Therefore the three symmetries are all conjugate to each other.

Thus this cycle structure class splits into two conjugacy classes:

$$\{(1\ 4)(2\ 5)(3\ 6)\},$$
$$\{(1\ 6)(2\ 5)(3\ 4),\ (1\ 2)(3\ 6)(4\ 5),\ (1\ 4)(2\ 3)(5\ 6)\}.$$

Finally, consider the cycle structure class

$$\{(2\ 6)(3\ 5),\ (1\ 3)(4\ 6),\ (1\ 5)(2\ 4)\}.$$

The three symmetries in this class are all reflections in axes that pass through two vertices. Hence for any pair of these symmetries there is a rotation of the hexagon that transforms a diagram illustrating one of the pair to a diagram illustrating the other. Therefore the three symmetries are all conjugate to each other. Thus this cycle structure class is a conjugacy class.

In summary, the conjugacy classes of $S(\hexagon)$ are as follows.

$$\{e\}$$
$$\{(1\ 2\ 3\ 4\ 5\ 6),\ (1\ 6\ 5\ 4\ 3\ 2)\}$$
$$\{(1\ 3\ 5)(2\ 4\ 6),\ (1\ 5\ 3)(2\ 6\ 4)\}$$
$$\{(1\ 4)(2\ 5)(3\ 6)\}$$
$$\{(1\ 6)(2\ 5)(3\ 4),\ (1\ 2)(3\ 6)(4\ 5),\ (1\ 4)(2\ 3)(5\ 6)\}$$
$$\{(2\ 6)(3\ 5),\ (1\ 3)(4\ 6),\ (1\ 5)(2\ 4)\}$$

(c) The symmetry group of the given modified regular hexagon is

$$\{e,\ (1\ 6)(2\ 5)(3\ 4),\ (1\ 3)(4\ 6),\ (1\ 4)(2\ 5)(3\ 6)\}.$$

This subgroup is not normal in $S(\hexagon)$ because it is not a union of conjugacy classes of $S(\hexagon)$. For example, the element $(1\ 3)(4\ 6)$ of the subgroup lies in the same conjugacy class as $(1\ 5)(2\ 4)$, but this symmetry is not an element of the subgroup.

Solution to Exercise E94

We use Strategy E6. There are many different ways to work out the conjugacy classes of $S(\text{doubletet})$. One method is given here.

The partition of $S(\text{doubletet})$ by cycle structure is as follows.

$$\begin{array}{l}\{e\}\\ \{(1\ 2),\ (1\ 3),\ (2\ 3),\ (4\ 5)\}\\ \{(1\ 2\ 3),\ (1\ 3\ 2)\}\\ \{(1\ 2)(4\ 5),\ (1\ 3)(4\ 5),\ (2\ 3)(4\ 5)\}\\ \{(1\ 2\ 3)(4\ 5),\ (1\ 3\ 2)(4\ 5)\}\end{array}$$

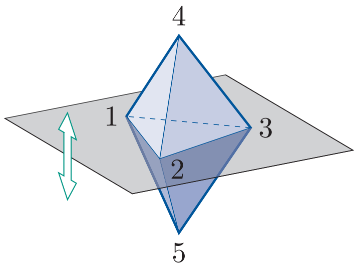
One conjugacy class is $\{e\}$.

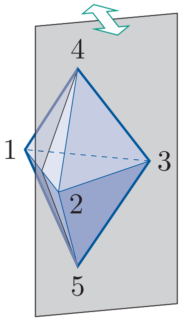
Now consider the cycle structure class

$$\{(1\ 2),\ (1\ 3),\ (2\ 3),\ (4\ 5)\}.$$

We can use the fact that the group $S(\triangle)$, with its usual representation as permutations of the vertex labels 1, 2 and 3, is a subgroup of $S(\text{doubletet})$. The elements $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ are all conjugate in $S(\triangle)$ (by the solution to Exercise E92), so they are all conjugate in $S(\text{doubletet})$.

The symmetry $(4\ 5)$ is the reflection in the plane passing through the vertices 1, 2 and 3, shown on the left below. Its fixed point set is the triangle with vertices 1, 2 and 3. The symmetry $(1\ 2)$ is the reflection in the plane passing through the vertices 3, 4 and 5, shown on the right below. Its fixed point set is the part of this plane lying within the double tetrahedron. There is no symmetry of the double tetrahedron that maps one of these two fixed point sets to the other, so by Theorem E34 the symmetries $(4\ 5)$ and $(1\ 2)$ are not conjugate in $S(\text{doubletet})$.





Thus the cycle structure class above splits into two conjugacy classes:

$$\{(1\ 2),\ (1\ 3),\ (2\ 3)\},\quad \{(4\ 5)\}.$$

Next consider the cycle structure class

$$\{(1\ 2\ 3),\ (1\ 3\ 2)\}.$$

Similarly to the above, the two elements of this class are conjugate in $S(\triangle)$, so they are also conjugate in $S(\text{doubletet})$. Thus this cycle structure class is a conjugacy class.

Now consider the cycle structure class

$$\{(1\ 2)(4\ 5),\ (1\ 3)(4\ 5),\ (2\ 3)(4\ 5)\}.$$

We know that in $S(\triangle)$ the element $(1\ 2\ 3)$ conjugates $(1\ 2)$ to $(2\ 3)$, so in $S(\text{doubletet})$ it must conjugate $(1\ 2)(4\ 5)$ to $(2\ 3)(4\ 5)$, since it will have no effect on the cycle $(4\ 5)$:

$$(1\ 2\ 3)\quad \begin{array}{l}(1\ 2)(4\ 5)\\ \ \downarrow\ \downarrow\ \ \ \downarrow\ \downarrow\\ (2\ 3)(4\ 5).\end{array}$$

Similarly, in $S(\triangle)$ the element $(1\ 2\ 3)$ conjugates $(2\ 3)$ to $(1\ 3)$, so in $S(\text{doubletet})$ it must conjugate $(2\ 3)(4\ 5)$ to $(1\ 3)(4\ 5)$:

$$(1\ 2\ 3)\quad \begin{array}{l}(2\ 3)(4\ 5)\\ \ \downarrow\ \downarrow\ \ \ \downarrow\ \downarrow\\ (3\ 1)(4\ 5) = (1\ 3)(4\ 5).\end{array}$$

Thus the cycle structure class above is a conjugacy class.

Finally consider the cycle structure class

$$\{(1\ 2\ 3)(4\ 5),\ (1\ 3\ 2)(4\ 5)\}.$$

We can argue in a similar way as for the previous cycle structure class. We know that in $S(\triangle)$ the element $(2\ 3)$ conjugates $(1\ 2\ 3)$ to $(1\ 3\ 2)$, so in $S(\text{doubletet})$ it must conjugate $(1\ 2\ 3)(4\ 5)$ to $(1\ 3\ 2)(4\ 5)$. Thus this cycle structure class is a conjugacy class.

In summary, the conjugacy classes of $S(\text{doubletet})$ are as follows.

$\{e\}$

$\{(1\ 2), (1\ 3), (2\ 3)\}$

$\{(4\ 5)\}$

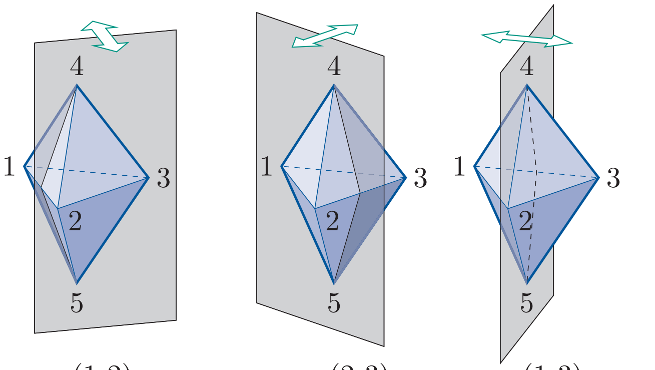
$\{(1\ 2\ 3), (1\ 3\ 2)\}$

$\{(1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5)\}$

$\{(1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\}$

(Here are some alternative methods that you could have used.

To work out that the three symmetries $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ are all conjugate, you can consider the geometric effects of these symmetries. They are all reflections in vertical planes, as shown below.



(1 2) (2 3) (1 3)

We would expect from these diagrams, or by considering the fixed point sets of these symmetries, that the rotation $(1\ 2\ 3)$ would conjugate $(1\ 2)$ to $(2\ 3)$ and conjugate $(2\ 3)$ to $(1\ 3)$, and we can confirm this by using the renaming method:

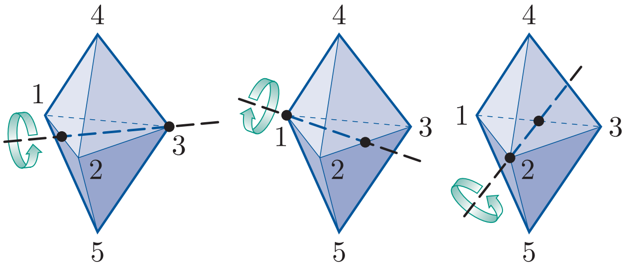
$$\begin{array}{cc} & (1\ 2) \\ (1\ 2\ 3) & \downarrow\downarrow \\ & (2\ 3), \end{array} \qquad \begin{array}{cc} & (2\ 3) \\ (1\ 2\ 3) & \downarrow\downarrow \\ & (3\ 1) = (1\ 3). \end{array}$$

Thus the three symmetries $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ are all conjugate.

To work out that the cycle structure class

$$\{(1\ 2)(4\ 5), (1\ 3)(4\ 5), (2\ 3)(4\ 5)\}$$

is a conjugacy class, again we can consider the effects of these symmetries. Each of them is a rotation through π about a horizontal axis, as shown below.



(1 2)(4 5) (2 3)(4 5) (1 3)(4 5)

We would expect from these diagrams, or by considering the fixed point sets of these symmetries, that the rotation $(1\ 2\ 3)$ would conjugate $(1\ 2)(4\ 5)$ to $(2\ 3)(4\ 5)$ and conjugate $(2\ 3)(4\ 5)$ to $(1\ 3)(4\ 5)$, and we can confirm this using the renaming method, as is done in the main solution above.

To work out that the cycle structure class

$$\{(1\ 2\ 3)(4\ 5), (1\ 3\ 2)(4\ 5)\}$$

is a conjugacy class, we can simply try conjugating the symmetry $(1\ 2\ 3)(4\ 5)$ by elements of $S(\text{doubletet})$ in turn (using the renaming method) to see if we can obtain the symmetry $(1\ 3\ 2)(4\ 5)$. It does not take long to find a suitable conjugating symmetry, as any of the symmetries $(1\ 2)$, $(1\ 3)$, $(2\ 3)$, $(1\ 2)(4\ 5)$, $(1\ 3)(4\ 5)$ and $(2\ 3)(4\ 5)$ will do. Note that finding the fixed point sets of the symmetries $(1\ 2\ 3)(4\ 5)$ and $(1\ 3\ 2)(4\ 5)$ is of no help, as the fixed point set of each of these two symmetries consists of the central point of the double tetrahedron alone, so every symmetry of the double tetrahedron maps the fixed point set of the first symmetry to the fixed point set of the second.)

Solution to Exercise E95

(a) We have

$$\begin{aligned}
&\begin{pmatrix}1&2\\0&1\end{pmatrix} D \begin{pmatrix}1&2\\0&1\end{pmatrix}^{-1}\\
&= \left\{\begin{pmatrix}1&2\\0&1\end{pmatrix}\begin{pmatrix}a&0\\0&d\end{pmatrix}\begin{pmatrix}1&2\\0&1\end{pmatrix}^{-1} : \begin{pmatrix}a&0\\0&d\end{pmatrix}\in D\right\}\\
&= \left\{\begin{pmatrix}1&2\\0&1\end{pmatrix}\begin{pmatrix}a&0\\0&d\end{pmatrix}\begin{pmatrix}1&2\\0&1\end{pmatrix}^{-1} : a,d\in\mathbb{R},\ ad\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&2d\\0&d\end{pmatrix}\begin{pmatrix}1&-2\\0&1\end{pmatrix} : a,d\in\mathbb{R},\ ad\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&-2a+2d\\0&d\end{pmatrix} : a,d\in\mathbb{R},\ ad\neq 0\right\}.
\end{aligned}$$

This subgroup is not equal to U because, for example,

$$\begin{pmatrix}1&0\\0&2\end{pmatrix}\in U,$$

since this matrix is upper triangular and invertible, but

$$\begin{pmatrix}1&0\\0&2\end{pmatrix}\notin \begin{pmatrix}1&2\\0&1\end{pmatrix} D \begin{pmatrix}1&2\\0&1\end{pmatrix}^{-1},$$

because there are no numbers $a,d\in\mathbb{R}$ such that

$$\begin{pmatrix}a&-2a+2d\\0&d\end{pmatrix} = \begin{pmatrix}1&0\\0&2\end{pmatrix}.$$

This is because if $a=1$ and $d=2$ then

$$-2a+2d = 2\neq 0.$$

(b) We have

$$\begin{aligned}
&\begin{pmatrix}1&1\\0&1\end{pmatrix} U \begin{pmatrix}1&1\\0&1\end{pmatrix}^{-1}\\
&= \left\{\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}^{-1} : \begin{pmatrix}a&b\\0&d\end{pmatrix}\in U\right\}\\
&= \left\{\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}^{-1} : a,b,d\in\mathbb{R},\ ad\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&b+d\\0&d\end{pmatrix}\begin{pmatrix}1&-1\\0&1\end{pmatrix} : a,b,d\in\mathbb{R},\ ad\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&-a+b+d\\0&d\end{pmatrix} : a,b,d\in\mathbb{R},\ ad\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&c\\0&d\end{pmatrix} : a,c,d\in\mathbb{R},\ ad\neq 0\right\}.
\end{aligned}$$

The final line in the manipulation above is correct because as the value of b varies through all the numbers in $\mathbb{R}$, so does the value of $-a+b+d$, so we can denote the top right entry simply by c, say, where $c\in\mathbb{R}$.

(Alternatively we could denote the top right entry by b, where $b\in\mathbb{R}$, but using a different variable may help to make the argument clearer.)

This subgroup is equal to U because the specification found above is exactly the same as the specification for U, except that the top right entry of the matrix is denoted by c instead of b, which does not make any difference to the set specified.

Solution to Exercise E96

(a) We have

$$\begin{aligned}
&\begin{pmatrix}1&3\\0&2\end{pmatrix} M \begin{pmatrix}1&3\\0&2\end{pmatrix}^{-1}\\
&= \left\{\begin{pmatrix}1&3\\0&2\end{pmatrix}\begin{pmatrix}a&b\\0&a\end{pmatrix}\begin{pmatrix}1&3\\0&2\end{pmatrix}^{-1} : \begin{pmatrix}a&b\\0&a\end{pmatrix}\in M\right\}\\
&= \left\{\begin{pmatrix}1&3\\0&2\end{pmatrix}\begin{pmatrix}a&b\\0&a\end{pmatrix}\begin{pmatrix}1&3\\0&2\end{pmatrix}^{-1} : a,b\in\mathbb{R},\ a\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&b+3a\\0&2a\end{pmatrix}\times\frac{1}{2}\begin{pmatrix}2&-3\\0&1\end{pmatrix} : a,b\in\mathbb{R},\ a\neq 0\right\}\\
&= \left\{\frac{1}{2}\begin{pmatrix}2a&b\\0&2a\end{pmatrix} : a,b\in\mathbb{R},\ a\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&\frac{1}{2}b\\0&a\end{pmatrix} : a,b\in\mathbb{R},\ a\neq 0\right\}\\
&= \left\{\begin{pmatrix}a&c\\0&a\end{pmatrix} : a,c\in\mathbb{R},\ a\neq 0\right\}.
\end{aligned}$$

The final line in the manipulation above is correct because as the value of b varies through all the numbers in $\mathbb{R}$, so does the value of $\frac{1}{2}b$, so we can denote the top right entry simply by c, say, where $c\in\mathbb{R}$.

(Alternatively we could denote the top right entry by b, where $b\in\mathbb{R}$.)

This subgroup is equal to M because the specification found above is exactly the same as the specification for M, except that the top right entry of the matrix is denoted by c instead of b, which does not make any difference to the set specified.

(b) We have

$$\begin{aligned}
&\begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix} M \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}^{-1} \\
&= \left\{ \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}^{-1} : \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M \right\} \\
&= \left\{ \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} 2 & -3 \\ 0 & -1 \end{pmatrix}^{-1} : a, b \in \mathbb{R},\ a \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} 2a & 2b-3a \\ 0 & -a \end{pmatrix} \times \left(-\frac{1}{2}\right) \begin{pmatrix} -1 & 3 \\ 0 & 2 \end{pmatrix} : \right. \\
&\qquad\qquad\qquad\qquad \left. a, b \in \mathbb{R},\ a \neq 0 \right\} \\
&= \left\{ -\frac{1}{2} \begin{pmatrix} -2a & 4b \\ 0 & -2a \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & -2b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\} \\
&= \left\{ \begin{pmatrix} a & c \\ 0 & a \end{pmatrix} : a, c \in \mathbb{R},\ a \neq 0 \right\}.
\end{aligned}$$

The final line in the manipulation above is correct because as the value of b varies through all the numbers in $\mathbb{R}$, so does the value of $-2b$, so we can denote the top right entry simply by c, say, where $c \in \mathbb{R}$.

(Alternatively we could denote the top right entry by b, where $b \in \mathbb{R}$.)

As in part (a), this subgroup is equal to M because the specification found above is exactly the same as the specification for M, except that the top right entry of the matrix is denoted by c instead of b, which does not make any difference to the set specified.

Solution to Exercise E97

We use Property B of Theorem E33.

The subgroup D is not a normal subgroup of GL(2), because, for example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in D \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2),$$

but

$$\begin{aligned}
&\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix},
\end{aligned}$$

which is not in D since it is not a diagonal matrix.

Solution to Exercise E98

(a) The set S is a *subset* of the group GL(2), because each matrix

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

in S has determinant

$$1 \times 1 - b \times 0 = 1$$

and is therefore invertible.

We show that the three subgroup properties hold for S (with the same binary operation as in GL(2), namely matrix multiplication).

SG1 Closure

Let $\mathbf{A}, \mathbf{B} \in S$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix},$$

for some $x, y \in \mathbb{R}$. So

$$\mathbf{AB} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}.$$

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = x + y \in \mathbb{R}$. So $\mathbf{AB} \in S$. Thus S is closed under matrix multiplication.

SG2 Identity

The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of GL(2) is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = 0$.

Thus $\mathbf{I} \in S$.

SG3 Inverses

Let $\mathbf{A} \in S$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

for some $x \in \mathbb{R}$. The inverse of $\mathbf{A}$ in GL(2) is

$$\mathbf{A}^{-1} = \frac{1}{1}\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}.$$

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = -x \in \mathbb{R}$. So $\mathbf{A}^{-1} \in S$. Thus S contains the inverse of each of its elements.

Since the three subgroup properties hold, S is a subgroup of GL(2).

(This solution is similar to the solution to Worked Exercise E8 in Section 2 of Unit E1. The subset Y of GL(2) defined there and the subset S of GL(2) defined here have similar – but not the same – definitions.)

(b) We use Property B of Theorem E33.

The subgroup S is not a normal subgroup of GL(2), because, for example,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in S \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}(2),$$

but

$$\begin{aligned} &\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \end{aligned}$$

which is not in S since (for example) its bottom right entry is not 1.

(c) The set S is a subset of the group U, because each matrix in it is upper triangular and has determinant 1 so is invertible. Also, S is a group under matrix multiplication, by part (a). Therefore S is a subgroup of U.

To show that S is normal in U, we use Property B of Theorem E33.

We have to show that for every matrix $\mathbf{A} \in S$ and every matrix $\mathbf{B} \in U$, we have $\mathbf{BAB}^{-1} \in S$. Let $\mathbf{A} \in S$ and let $\mathbf{B} \in U$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$$

for some $x, r, s, u \in \mathbb{R}$ where $ru \neq 0$.

We have

$$\begin{aligned} \mathbf{BAB}^{-1} &= \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} r & s \\ 0 & u \end{pmatrix}^{-1} \\ &= \begin{pmatrix} r & rx+s \\ 0 & u \end{pmatrix} \times \frac{1}{ru}\begin{pmatrix} u & -s \\ 0 & r \end{pmatrix} \\ &= \frac{1}{ru}\begin{pmatrix} ru & -rs+r^2x+rs \\ 0 & ru \end{pmatrix} \\ &= \begin{pmatrix} 1 & rx/u \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

This matrix is of the form

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

with $b = rx/u \in \mathbb{R}$. Hence $\mathbf{BAB}^{-1} \in S$.

Thus S is a normal subgroup of U.